Informationssikkerhed – vejledning for sundhedsvæsenet

Informationssikkerhed – vejledning for sundhedsvæsenet

Sundhedsstyrelsen

Islands Brygge 67

2300 København S

URL: http://www.sst.dk

Kategori: **Vejledning, A. Lovbaseret**

Emneord: Informationssikkerhed; persondataloven; sundhedsloven; samtykke; 'sige-fra-model'; personoplysninger; patientdata; sikkerhedsbekendtgørelse; sikringsforanstaltning; it-sikkerhed

Sprog: Dansk

Version: 0.96

Versionsdato: 2007-10-30

Elektronisk ISBN: 978-87-7676-577-4

Format: pdf

Udgivet af: Sundhedsstyrelsen

Forord

En vigtig del af informationssikkerhed i sundhedsvæsenet vedrører beskyttelse af patienters helbredsoplysninger.

De nye regler i sundhedsloven om sundhedspersoners adgang til elektroniske systemer i forbindelse med behandling af patienter er udtryk for en afvejning af på den ene side effektivitet i patientbehandlingen og på den anden side patienternes krav på fortrolig behandling af data.

Ved at give sundhedspersonalet en hurtig adgang til relevante oplysninger om de patienter, der er i behandling, udnyttes de fordele som elektroniske informationssystemer indebærer, men samtidig skal den enkelte patient kunne føle sig tryg ved, at de ansatte i sundhedsvæsenet har adgang til patientdata.

Sigtet med denne vejledning er at oplyse nærmere om lovregler og konkrete sikringsforanstaltninger til opnåelse af den nødvendige informationssikkerhed i sundhedsvæsenet.

Enhed

Måned

Navn

Titel

Indhold

1 Indledende del

1.1 Baggrund

I juli 2002 udgav Sundhedsstyrelsen 'IT-sikkerhedsvejledning for sygehuse'. Vejledningen var et element i 'National strategi for sygehusvæsenet 2000-2002' og indeholdt Sundhedsstyrelsens anvisninger på, hvorledes lovgivningens krav på området opfyldes, og hvorledes sikkerheden omkring den daglige brug af it på de danske sygehuse kunne opretholdes.

Der er en række forhold, som har ændret sig siden 2002. Ændringerne giver anledning til, at sikkerhedsvejledningen bliver opdateret og udvides til at dække hele sundhedsvæsenet.

Der er sket en øget udbredelse og brug af it-støtte til arbejdet i sundhedsvæsenet. EPJ-Observatoriet oplyser[1], at EPJ-sengedækningen på hospitalerne siden 2002 er vokset fra 8 % til 47 % i 2006, og andelen af elektroniske henvisninger fra de praktiserende læger er ifølge MedCom siden 2002 vokset fra 12 % til 65 % i 2007[2].

'National IT-strategi for sundhedsvæsenet 2003-2007' anfører i afsnittet 'Informationssikkerhed', at der løbende er behov for at stille passende vejledningsmateriale om dette emne til rådighed for hele sundhedsvæsenet. Strategien er under revision, og afklaring af sikkerhedsaspekterne vedr. it-anvendelse er en væsentlig forudsætning for dette arbejde.

Folketinget vedtog i maj 2006 en ny autorisationslov[3] bl.a. med bestemmelser om journalføring, der regulerer journalføringspligten, opbevaring, videregivelse og overdragelse af patientjournaler m.v.

I april 2007 blev nye regler om sundhedspersoners adgang til elektroniske patientjournaler vedtaget. Reglerne findes i sundhedslovens[4] §§ 42 a og 42 b[5], der trådte i kraft den 1. oktober 2007. De nye regler gælder såvel for fremtidige elektroniske systemer, som for de elektroniske systemer, der anvendes i sundhedsvæsenet i dag. Lovændringerne medfører ikke en pligt for sundhedsvæsenet til at etablere elektroniske patientjournaler i sundhedsvæsenet. Formålet med de nye regler er alene at fastlægge de juridiske rammer for sundhedspersoners adgang til at indhente elektroniske helbredsoplysninger m.v. i forbindelse med behandling af patienter.

Regeringen, Danske Regioner og KL (Kommunernes Landsforening) har i samarbejde i juni 2007 udarbejdet en digitaliseringsstrategi for det offentlige[6] med tre overordnede strategiske indsatsområder: Bedre digital service, øget effektivisering og stærkere forpligtende samarbejde. Øget digitalisering skal i høj grad baseres på øget samarbejde og koordinering i form af fx fælles standarder og dataadgang på tværs af sektorer, myndigheder og myndighedsniveauer.

I store dele af den offentlige sektor implementeres nu den danske standard for informationssikkerhed, DS 484[7]. Denne standard angiver, hvordan det er muligt at gå frem for at opnå et velovervejet niveau for informationssikkerhed.

1.2 Formål

Vejledningens formål er at præcisere lovmæssige krav og konkretisere sikringsforanstaltninger og -overvejelser for derved at opnå og fastholde informationssikkerheden i sundhedsvæsenet.

Det er tillige vejledningens formål at fastslå og tydeliggøre at informationssikkerhed er et ledelsesansvar.

1.3 Målgrupper

Den primære målgruppe for vejledningen er alle ledere i sundhedsvæsenet, herunder privatpraktiserende sundhedspersoner som fx fysioterapeuter, fodterapeuter, alment praktiserende læger og andre speciallæger.

Den sekundære målgruppe er it-leverandører til sundhedsvæsenet og it-relaterede medarbejdere i sundhedsvæsenet, fordi de er involveret i udførelsen af de teknisk prægede sikringsforanstaltninger.

Patienterne bliver i tiltagende grad brugere af informationer. Patienterne opfattes ikke som en målgruppe for vejledningen, da de ikke har ansvaret for opretholdelse af informationssikkerheden i sundhedsvæsenet.

1.4 Ledelsens ansvar

Informationssikkerhed er et ledelsesansvar[7]. Ledelsen har derfor til opgave at træffe beslutning om:

- målsætning for informationssikkerheden – på det strategiske niveau
- valg af metoder, allokering af ressourcer samt placering af beføjelser og ansvar – på det taktiske niveau
- opfølgning på trufne beslutningers gennemførelse og sikring af nødvendige sikkerhedsdokumentation - på det operationelle niveau

Ledelsens valg af informationssystemer og tilrettelæggelse af arbejdsprocedurer og -opgaver skal gøre det let for medarbejderne at opretholde informationssikkerheden.

Uanset om informationssystemers drift varetages helt eller delvis af en ekstern part, stilles der samme krav til informationssikkerheden.

1.5 Læsevejledning

1.5.1 Indhold

Vejledningen henvender sig til både små og store behandlingsenheder i sundhedsvæsenet. Målet med vejledningen er at give et redskab til forståelsen af begrebet informationssikkerhed. Endvidere er målet at angive, hvornår lovgivningen forpligter sundhedsvæsenet til at foretage konkrete sikringsforanstaltninger bl.a. med hen-

blik på at opnå informationssikkerhed i sundhedsvæsenet. Vejledningen omtaler således regler fra relevante love og tager udgangspunkt i den danske standard for informationssikkerhed, DS 484[7]. Vejledningen supplerer DS 484 og beskriver de særlige forhold, der gør sig gældende i sundhedsvæsenet. I hovedafsnittet 'Konkret del' er hvert sikringsområde struktureret som i DS 484, inklusiv en beskrivelse af formålet med beskyttelsen. Afsnittet omtaler særlige forhold og regler i sundhedsvæsenet. I afsnittet gentages ikke detaljeret beskrivelser af sikringsforanstaltninger og deres implementeringsretningslinier, der er lige så relevante for sundhedssektoren som for andre samfundssektorer.

I vejledningen benyttes udtrykket 'EPJ-system' som samlet betegnelse for alle elektroniske systemer, der indeholder helbredsoplysninger og andre patientdata. Der er tale om systemer indeholdende data, der er indsamlet til det formål at understøtte den sundhedsfaglige behandling af de registrerede patienter eller til formål, der ikke er uforenelige hermed.

Brugen af termerne politikker, retningslinjer og procedurer er i overensstemmelse med DS 484.

Referencer er indsat med talhenvisninger til Bilag 2: Referenceliste, mens fodnoter er alfabetisk markeret og placeret nederst på den relevante side.

1.5.2 Struktur

Vejledningen består af tre dele:

- 'Indledende del', som samlet forklarer baggrunden for vejledningen og dens kontekst
- 'Generel del', som fokuserer på de generelle spørgsmål inden for informationssikkerhed, der er relevante for sundhedsvæsenet
- 'Konkret del', som omtaler konkrete sikringsforanstaltninger og forhold som er særligt relevante for sundhedsvæsenet samt giver referencer til lovbestemmelser

For det statslige område er det obligatorisk at følge den danske standard for informationssikkerhed DS 484. Regeringen, Danske Regioner og KL skriver i den fællesoffentlige digitaliseringsstrategi[6] side 12, at standarden DS 484 skal udbredes til hele den offentlige sektor.

Vejledningen har to bilag:

Bilag 1: Ord- og begrebsforklaring er en alfabetisk ord- og begrebsliste med forklaring på ord og begreber, der benyttes i vejledningen.

Bilag 2: Referenceliste er en liste over de kilder, vejledningen henviser til.

2 Generel del

2.1 Vejledningens anvendelsesområder

2.1.1 Hele sundhedsvæsenet

Vejledningen er rettet mod hele sundhedsvæsenet. Sundhedsvæsenets opgaver udføres af regionernes sygehusvæsen, praktiserende sundhedspersoner, kommunerne og øvrige offentlige og private institutioner m.v.[a] Vejledningen retter sig således bl.a. mod:

- den kommunale hjemmesygepleje og –genoptræning
- offentlige hospitaler
- private klinikker og privathospitaler
- praktiserende læger (almenmedicinere såvel som andre speciallæger)
- fysioterapeuter og andre praktiserende sundhedspersoner

2.1.2 Informationssystemer

Vejledningen omfatter alle typer af informationssystemer i sundhedsvæsenet, herunder it-systemer, der indeholder helbredsoplysninger og andre patientdata, der er indsamlet til det formål at understøtte den sundhedsfaglige behandling af de registrerede patienter eller til formål, der ikke er uforenelige hermed. Derfor er fx personaleadministrative systemer og andre rent administrative systemer ikke omfattet.

Vejledningen omfatter systemer, der indeholder patientdata og personhenførbare data, fx laboratoriesystemer, patientadministrative systemer, kliniske kvalitetsdatabaser og medicoteknisk udstyr.

Vejledningen omhandler også oplysninger som fx papiroplysninger, røntgenbilleder, videooptagelser, oversigtstavler m.v.

2.2 Informationssikkerhed

Formålet med informationssikkerhed er at beskytte informationer.

Information og informationssystemer er aktiver for en organisation på samme måde som produktionsudstyr, kapital, lagervarer, medarbejdere og andre ressourcer. Disse aktiver skal beskyttes, for at en organisation kan opretholde sine aktiviteter. I sundhedsvæsenet er der desuden en række juridiske krav til informationssikkerheden, som skal opfyldes. Det gælder om at implementere passende sikringsforanstaltninger for at opnå et informationssikkerhedsniveau, der matcher organisationens vurdering af sårbarhed over for mulige ”trusler” og konsekvens heraf. Med

[a] Sundhedslovens § 3, stk. 2

trusler menes de hændelser, som kan forhindre organisationens aktiviteter eller påvirke organisationen negativt.

Informationssikkerhed anses for at bestå af 'tilgængelighed', 'integritet' og 'fortrolighed'. Man kan tale om, at der med en vis grad af informationssikkerhed menes, hvor lettilgængelig information er for rette vedkommende, samt hvor godt den samme information er beskyttet mod ændring eller tab (integritet) og hvor godt den er beskyttet mod uvedkommendes adgang (fortrolighed).

Oplysninger på papir er også omfattet af begrebet 'informationssikkerhed' og gøres til genstand for sikringsforanstaltninger.

2.3 Lovgrundlag

2.3.1 Persondataloven

Når en offentlig myndighed eller en privat organisation m.v. behandler personoplysninger helt eller delvist ved hjælp af elektronisk databehandling, eller ikke-elektronisk behandler personoplysninger, der er eller vil blive indeholdt i et register, er der nogle generelle og grundlæggende krav i persondataloven[8], som altid skal være opfyldt. Persondataloven indeholder endvidere regler om den registreredes rettigheder og behandlingssikkerhed.

De nye regler i sundhedsloven[5]om indhentning af elektroniske helbredsoplysninger m.v. skal ses i sammenhæng med de eksisterende bestemmelser i persondataloven og de regler, der er fastsat i medfør heraf. Disse regler gælder fortsat. Det følger således af de persondataretlige regler, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at blandt andet helbredsoplysninger hændeligt eller ulovligt tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab (ubeføjet udbredelse), misbruges eller i øvrigt behandles i strid med loven. Heri ligger bl.a., at alene sundhedspersoner, der har et sagligt behov for at få adgang til EPJ-systemer, må autoriseres hertil, og at den enkelte sundhedsperson alene må autoriseres til anvendelser (og derfor få teknisk adgang til oplysninger), som vedkommende har behov for[b].

Sundhedslovens bestemmelser om sundhedspersoners juridiske adgang til indhentning af oplysninger i EPJ-systemer regulerer ikke direkte spørgsmålet om teknisk adgang. Spørgsmålet om, i hvilket omfang der vil være tale om ubeføjet udbredelse af oplysninger fra et EPJ-system, afhænger imidlertid af reglerne om, hvilke oplysninger de forskellige grupper af sundhedspersoner må indhente. De juridiske betingelser for indhentning vil således få betydning for, i hvilket omfang sundhedspersoner må få teknisk adgang (adgangsrettigheder) til oplysningerne efter persondataloven.

De nærmere regler vedr. behandlingssikkerhed er fastsat i Justitsministeriets bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen)[9] og beskrevet i Datatilsynets vejledning om sikkerhedsforanstaltninger til beskyttelse af

[b] Persondatalovens § 41, stk. 3

personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsvejledningen)[10]. Datatilsynet anbefaler[11], at vejledningens regler for den offentlige forvaltning anvendes på private organisationer m.v.

De persondataretlige regler om behandlingssikkerhed, autorisation og adgangskontrol vil blive nærmere behandlet i forbindelse med beskrivelsen af informationssikkerhedens emneområder, jf. pkt. 3.8.

2.3.2 Sundhedsloven

2.3.2.1 Sundhedslovens kapitel 9

Reglerne om sundhedspersoners tavshedspligt, videregivelse og indhentning af helbredsoplysninger m.v. findes i sundhedslovens kapitel 9.

Begreberne indhentning og videregivelse er afgørende for, hvilke af reglerne i sundhedsloven der finder anvendelse. Sundhedslovens §§ 42 a og 42 b giver adgang til indhentning af helbredsoplysninger m.v. ved opslag i elektroniske systemer i forbindelse med behandling af patienter. Sundhedslovens §§ 41 og 42 gælder for videregivelse i øvrigt af helbredsoplysninger m.v. i forbindelse med behandling af patienter, og sundhedslovens §§ 43 - 49 gælder for videregivelse til andre formål end behandling, fx videregivelse fra en sundhedsperson til et privat forsikringsselskab. Se i øvrigt Bilag 1: Ord- og begrebsforklaring for en nærmere afgrænsning af begreberne.

Reglerne om videregivelse af oplysninger er en i det væsentlige uændret videreførelse af de tidligere gældende regler i lov om patienters retsstilling, mens reglerne om indhentning af oplysninger fra elektroniske systemer er nye regler, som trådte i kraft den 1. oktober 2007. De nye reglers baggrund, anvendelsesområde m.v. er nærmere beskrevet under pkt. 2.3.2.3.

2.3.2.2 Sundhedslovens regler om indhentning af oplysninger

Før den 1. oktober 2007 måtte sundhedspersoner som udgangspunkt kun foretage opslag i et EPJ-system med patientens samtykke. I særlige tilfælde kunne der dog foretages opslag uden patientsamtykke, men opslaget var så bl.a. betinget af tilladelse til videregivelse fra den sundhedsperson, der var i besiddelse af oplysningen. Det har derfor været nødvendigt at vedtage specifikke regler om adgangen til oplysninger i EPJ-systemer for at sikre, at anvendelse af EPJ-systemer fremover kan ske effektivt og hurtigt. De nye regler bygger på en sige-fra-model, som indebærer, at sundhedspersonen – når betingelserne i øvrigt er opfyldt - kan foretage opslag i et EPJ-system, medmindre patienten siger fra.

Reglerne trådte i kraft den 1. oktober 2007, hvorefter der således er et specifikt regelsæt, der omhandler indhentning af helbredsoplysninger m.v. ved opslag i elektroniske systemer.

Anvendelsesområdet for de nye regler

Anvendelsesområdet for de nye regler i sundhedsloven er indhentning af oplysninger i det danske sundhedsvæsen ved opslag i elektroniske systemer, der indeholder helbredsoplysninger og andre personoplysninger, der er indsamlet til det formål at

understøtte den sundhedsfaglige behandling af de registrerede patienter eller til formål, der ikke er uforenelige hermed, fx Landspatientregisteret. Papirjournaler (manuelle patientjournaler) er ikke omfattet af reglerne. De nye regler regulerer opslag i elektroniske systemer, (praksissystemer, sygehusenes og hjemmesygeplejens elektroniske systemer etc.), medmindre der findes særlige regler om adgang til bestemte systemer, som fx den Personlige Elektroniske Medicinprofil, som reguleres af sundhedslovens § 157.

Opslag i personaleadministrative systemer og andre rent administrative systemer er ikke omfattet af reglerne, mens fx indhentning af oplysninger fra medicoteknisk udstyr, der lagrer personhenførbare data om patienter, er omfattet. Reglerne finder ligeledes anvendelse på opslag i laboratoriesystemer, patientadministrative systemer og kliniske kvalitetsdatabaser, der indeholder patientdata.

Vejledningen adresserer ikke spørgsmålet om adgangen til oplysninger om sundhedspersoners arbejdsindsats og resultater.

Reglerne regulerer kun sundhedspersoners opslag i elektroniske systemer i forbindelse med aktuel patientbehandling. Ved sundhedspersoner forstås personer, der er (sundhedsfagligt) autoriserede i henhold til særlig lovgivning[3] til at varetage sundhedsfaglige opgaver, og personer, der handler på disses ansvar[c]. Det er en betingelse, at den ansatte aktivt udfører eller medvirker ved patientbehandlingen for at kunne defineres som en sundhedsperson. Det afhænger af en konkret vurdering, om en ansat i sundhedsvæsenet udfører opgaver, der gør, at vedkommende kan defineres som sundhedsperson. Elever og studerende vil også kunne være sundhedspersoner, hvis ovennævnte betingelser er opfyldt.

De nye regler regulerer som nævnt adgangen til at indhente helbredsoplysninger i EPJ-systemer i forbindelse med patientbehandling. De supplerer og erstatter de gældende videregivelsesregler i sundhedsloven. Når en sundhedsperson efter den 1. oktober 2007 indhenter elektroniske helbredsoplysninger i forbindelse med aktuel behandling, vil dette således alene være reguleret af sundhedslovens § 42 a.

Videregivelse i øvrigt af oplysningerne reguleres fortsat af de øvrige regler i sundhedslovens kapitel 9. I de tilfælde, hvor en sundhedsperson har behov for at få adgang til helbredsoplysninger, som sundhedspersonen ikke kan indhente, fordi betingelserne for indhentning ikke er opfyldt, kan der således fortsat ske en videregivelse af oplysningerne til denne sundhedsperson efter de almindelige videregivelsesregler i sundhedslovens kapitel 9. Det betyder, at den pågældende sundhedsperson kan få videregivet oplysningerne i overensstemmelse med de almindelige videregivelsesregler fra en anden sundhedsperson, fx en læge, der har adgang til de relevante oplysninger i EPJ-systemet.

De hidtidige videregivelsesregler vil fortsat regulere sundhedspersoners videregivelse af helbredsoplysninger i de tilfælde, hvor der ikke er tale om indhentning af oplysninger via opslag i EPJ-systemer, fx fra papirbaserede journaler. Der henvises til Bilag 1: Ord- og begrebsforklaring vedr. begreberne videregivelse og indhentning.

[c] Sundhedslovens § 6

Den nærmere betydning af reglerne i relation til informationssikkerhed og i forbindelse med implementering af sikringsforanstaltninger beskrives i vejledningens konkrete del.

2.3.2.3 Adgangsbetingelser efter indhentningsreglerne

Generelle adgangsbetingelser

For alle de sundhedspersoner – uanset faggruppe – der har juridisk adgang til et EPJ-system[d], gælder følgende 3 betingelser for at fortage opslag i EPJ-systemet i forbindelse med patientbehandling:

1) Der må alene indhentes oplysninger, når det er nødvendigt i forbindelse med aktuel behandling af en patient. Det vil sige, at der skal være en patient-behandler relation.

2) Der må alene indhentes oplysninger i fornødent omfang. Heri ligger, at hvis systemet er indrettet således, at sundhedspersonen ved opslag i systemet først præsenteres for en oversigt af de oplysninger, som vil kunne søges frem fra et dybereliggende niveau i systemet, må den pågældende sundhedsperson kun slå op på de oplysninger, som det vurderes, der er et fagligt behov for at indhente. Hvis det er teknisk muligt at begrænse adgangen til fx kategorier af oplysninger eller bestemte oplysninger, så vil lovgivningens betingelse om, at sundhedspersoner kun skal have adgang i fornødent omfang, medføre, at sundhedspersoner kun kan få teknisk adgang til de – kategorier af – oplysninger, som vedkommende har behov for.

3) Patienten må ikke have udnyttet sin ret til at sige fra over for indhentning af helbredsoplysninger. Patientens tilkendegivelse om, at patienten ikke ønsker, at der indhentes oplysninger fra EPJ-systemet, kan ske mundtligt eller skriftligt, og skal journalføres i patientens EPJ. Patientens ret til at sige fra over for indhentning af oplysninger fra EPJ-systemet gør, at EPJ-systemerne skal kunne håndtere, at der teknisk blokeres for opslag i overensstemmelse med patientens ønsker.

De 3 adgangsbetingelser gælder ikke i fuldt omfang, hvis sundhedspersonen indhenter oplysninger efter den såkaldte værdispringsregel, se nedenfor.

De konkrete adgangsbetingelser

Læger, sygehusansatte tandlæger og medicinstuderende får en bred adgang til EPJ-systemer, da de får adgang til at foretage opslag i historiske og aktuelle oplysninger og adgang til opslag på tværs af sektorer og faggrænser, hvis det er nødvendigt (og teknisk muligt). Lægers, sygehusansatte tandlægers og medicinstuderendes adgang til EPJ-systemer er således alene begrænset af de 3 generelle betingelser.

Læger, sygehusansatte tandlæger og medicinstuderende kan endvidere i medfør af sundhedsloven[e], i forbindelse med behandling af patienter foretage opslag i EPJ-systemer med patientens samtykke, når opslaget ikke er nødvendigt i forbindelse

[d] Sundhedslovens § 42 a

[e] Sundhedslovens § 42 a, stk. 6 og stk. 8

med den igangværende behandling af patienten, eller når betingelserne for at foretage opslag efter værdispringsreglen ikke er opfyldt. Ønsker patienten fx, at lægen indhenter yderligere oplysninger om patienten fra et EPJ-system, end de oplysninger, der er nødvendige til brug for den igangværende behandling, vil lægen med patientens samtykke kunne indhente sådanne oplysninger. Patientens samtykke skal journalføres i patientens EPJ[f]. EPJ-systemerne skal således kunne administrere og ajourføre patientens samtykke.

Andre sundhedspersoner end læger, sygehusansatte tandlæger og medicinstuderende får en mere begrænset adgang til EPJ-systemer, idet der ud over de 3 generelle betingelser som udgangspunkt gælder yderligere to betingelser for at indhente oplysninger fra et EPJ-system:

a) adgangen skal teknisk være begrænset til patienter i behandling på samme behandlingsenhed (organisatorisk tilknytning)

b) det er kun tilladt at indhente oplysninger om aktuel behandling

De to betingelser gælder ikke, hvis der er tale om et lukket system[g], eller der er tale om en sundhedsperson med tilladelse til en bredere adgang til opslag fra behandlingsstedets ledelse[h], se nedenfor.

Ad a): Kravet om tilknytning til samme behandlingsenhed indebærer et krav om, at sundhedspersonen og patienten er tilknyttet samme behandlingsenhed, hvor der udføres sundhedsfaglig virksomhed. Denne tilknytning skal afspejles i den pågældende sundhedspersons systemtekniske adgang. Ved udtrykket behandlingsenhed forstås sygehus, sygehusafdeling, afsnit, klinik eller lign., idet kravet om organisatorisk tilknytning skal administreres så snævert, som det teknisk er muligt.

Ad b): Ved oplysninger om aktuel behandling forstås oplysninger registreret eller indhentet efter en bestemt dato, fx henvisningsdatoen, indlæggelsesdatoen eller datoen for iværksættelsen af et ambulant forløb. Ved genindlæggelser inden for en kortere periode for samme helbredsproblem, hvor indlæggelserne må betragtes som en del af et sammenhængende behandlingsforløb, vil oplysninger om de tidligere indlæggelser ligeledes være oplysninger om aktuel behandling. En sundhedsperson, der foretager opslag i elektroniske systemer, må således foretage en vurdering af, om de elektroniske helbredsoplysninger, der søges indhentet, vil være oplysninger om aktuel behandling.

Betingelsen i § 42 a, stk. 2, om, at gruppen af andre sundhedspersoner kun må indhente oplysninger om aktuel behandling, indebærer ikke et krav om, at patienten fysisk skal være til stede i behandlingsenheden for der må indhentes oplysninger om vedkommende. Bliver en patient henvist fra en privatpraktiserende læge til behandling på et sygehus, vil disse sundhedspersoner således forud for patientens fremmøde kunne indhente de nødvendige, aktuelle oplysninger til brug for den kommende behandling

[f] Jf. sundhedslovens § 42 b

[g] Sundhedslovens § 42 a, stk. 3

[h] Sundhedsloven § 42 a, stk. 4

Begrænsningen indebærer, at de pågældende sundhedspersoners adgangsrettigheder datasikkerhedsmæssigt så vidt muligt skal administreres med henblik på at sikre, at historiske oplysninger er teknisk utilgængelige for de pågældende. De to betingelser behandles mere indgående i pkt. 3.8.

Lukkede systemer

Der findes en særlig regel[i] for såkaldt lukkede systemer. Herved forstås behandlingssteders elektroniske systemer, der kun indeholder oplysninger til brug for behandling, som gives på det pågældende behandlingssted. Der er tale om teknisk helt afgrænsede elektroniske systemer, hvorfra der ikke er direkte adgang til oplysninger fra andre, eksterne elektroniske patientsystemer, og hvortil der ikke kan indføres data direkte fra andre, eksterne elektroniske patientsystemer. Et eksempel herpå kan være en kiropraktor- eller fodterapeutklinik med egne elektroniske systemer, hvortil der ikke er direkte, elektronisk adgang for andre end de ansatte på klinikken.

I sådanne tilfælde vil der være behov for, at de ansatte sundhedspersoner kan få adgang til såvel oplysninger om aktuel behandling som historiske data. Derfor har alle sundhedspersoner på det pågældende behandlingssted fået juridisk adgang til at foretage opslag i både historiske og aktuelle patientdata. Det gælder dog ikke, hvis der er en læge eller en sygehusansat tandlæge ansat på det pågældende behandlingssted, idet denne i givet fald vil kunne foretage de nødvendige opslag og i fornødent omfang videregive oplysningerne efter de almindelige videregivelsesregler.

Begrebet 'lukket system' skal ikke forstås som et system med en fysisk afgrænsning, men derimod som en logisk afgrænsning. Et EPJ-system, som deler patientdata mellem to behandlingssteder er ikke et 'lukket system', da personalet på to behandlingssteder har adgang til oplysningerne i EPJ-systemet.

Tilladelse fra behandlingsstedets ledelse til en bredere adgang til opslag

Ledelsen på et behandlingssted har adgang til at træffe beslutning om, at enkelte eller grupper af sundhedspersoner, der er ansat på det pågældende behandlingssted, får juridisk adgang[j] til at foretage opslag i EPJ-systemer i samme omfang som læger og sygehusansatte tandlæger, hvis der er et behov herfor. Ledelsen på behandlingsstedet kan således sikre den fornødne fleksibilitet i reguleringen af adgangen til et EPJ-system ved at udpege de nøglepersoner, der har brug for en bredere adgang til EPJ-oplysninger og tildele dem den fornødne tekniske adgang. Tilladelsen til en bredere adgang til opslag kan kun gives til sundhedspersoner, der har behov for at kunne foretage opslag i samme omfang som læger og sygehusansatte tandlæger med henblik på at kunne varetage de funktioner og opgaver, vedkommende er beskæftiget med. Beslutninger om tilladelse til en bredere adgang til opslag skal gøres offentligt tilgængelig, fx på behandlingsstedets hjemmeside.

Det bemærkes, at det er op til den øverste ledelse i den enkelte forvaltningsmyndighed, herunder fx et regionsråd, hvorvidt man vil fastsætte overordnede retningslinier for, hvordan ledelsen på et behandlingssted – inden for lovens rammer – kan

[i] Sundhedsloven § 42 a, stk. 3

[j] Sundhedsloven § 42 a, stk. 4

udmønte muligheden for, at enkelte eller grupper af sundhedspersoner ansat på det pågældende behandlingssted, får en bredere adgang til opslag i EPJ-systemer.

Sekretærer

Sekretærer kan yde teknisk bistand til opslag i et EPJ-system under en sundhedspersons ansvar[k]. Sekretærernes adgang indebærer såvel en adgang til at yde teknisk bistand til at indhente oplysninger som en adgang til at yde teknisk bistand til at indtaste oplysninger i overensstemmelse med den ansvarlige sundhedspersons anvisninger herfor. Sekretæren kan alene yde teknisk bistand til opslag, som vedkommende sundhedsperson har juridisk adgang til at foretage, jf. ovenfor. Sekretærens adgang til at foretage opslag og indtaste oplysninger i EPJ-systemer afhænger således af, hvordan arbejdsprocedurerne er tilrettelagt på det enkelte behandlingssted, og hvilke opgaver sekretæren i den forbindelse er ansat til at udføre under ansvar af de relevante sundhedspersoner.

Værdispringsreglen

Sundhedspersoner kan indhente oplysninger efter den såkaldte værdispringsregel[l]. En sundhedsperson kan indhente oplysninger efter denne regel, hvis

1) indhentningen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke kan varetage sine interesser, sundhedspersonen eller andre patienter, og

2) sundhedspersonen er enten

> a) en læge, sygehusansat tandlæge eller medicinstuderende eller en sundhedsperson med tilladelse til bred adgang til opslag i EPJ-systemer fra ledelsen på et behandlingssted, eller
>
> b) en sundhedsperson, der foretager opslag i et EPJ-system, hvori adgangen for den pågældende sundhedsperson teknisk er begrænset til de patienter, der er i behandling på samme behandlingssted eller
>
> c) en sundhedsperson, der foretager opslag i et lukket elektronisk system.

I sådanne situationer vil kravet om aktuel behandling ikke altid være opfyldt, men der vil være andre vægtige grunde, der legitimerer opslaget. Derfor er det ikke et krav, at betingelsen om at der skal være etableret et patient-behandlerforhold, og at der alene må indhentes oplysninger, når det er nødvendigt i forbindelse med aktuel behandling af en patient, er opfyldt. Der er ikke mulighed for at sige fra over for indhentning af oplysninger, idet der som nævnt er tale om en værdispringsregel, hvor opslaget er legitimeret af andre vægtige grunde. Derfor skal betingelsen om, at patienten ikke må have udnyttet sin ret til at sige fra over for indhentning af helbredsoplysninger ikke være opfyldt ved opslag efter værdispringsreglen.

---

[k] Sundhedsloven § 42 a, stk. 9

[l] Sundhedsloven § 42 a, stk. 5

Indhentning efter værdispringsreglen kan kun ske i de situationer, der er opregnet i sundhedslovens § 42 a, stk. 5, hvor der foreligger særligt tungtvejende grunde, som overstiger patientens ret til fortrolighed. Værdispringsreglen kan for eksempel være relevant i situationer, hvor en person er blevet udsat for smitte (for eksempel ved at have fået en stikskade) fra en person, som formodes at have smitsom leverbetændelse.

Generelt afhænger det således af den ansattes organisatoriske rolle eller arbejdsfunktioner og tilknytning til en bestemt del af organisationen, hvilken information vedkommende kan autoriseres til at få adgang til. Se tabellen nedenfor.

:	Roller			
	Læge, sygehusansat tandlæge og medicinstuderende samt sundhedsperson med tilladelse fra behandlingsstedets ledelse	*Andre sundhedspersoner, herunder studerende*	*Sekretær (yder teknisk bistand – ikke sundhedsperson)*	
Supplerende betingelser	Dataomfang - hvilke oplysninger må indhentes *Generelle betingelser: Der må alene indhentes oplysninger:* *1) når det er nødvendigt ifm. aktuel behandling af en patient* *2) i fornødent omfang*			Samtykke/ sige-fra adgang
Supplerende betingelser for integrerbare og tilgængelige systemer	Både oplysninger om aktuel og historisk behandling	Kun oplysninger om: 1) Aktuel behandling 2) Om patienter i behandling på samme behandlingsenhed (organisatorisk tilknytning)	De oplysninger, som den sundhedsperson, sekretæren udfører teknisk bistand for, har adgang til	***Patienten kan sige fra***
Supplerende betingelser for lukkede systemer § 42 a, stk. 3[m]	Både oplysninger om aktuel og historisk behandling	a) Både oplysninger om aktuel og historisk behandling på det behandlingssted, hvor sundhedspersonen er ansat, hvis der ikke er ansat en læge eller sygehusansat tandlæge på behandlingsstedet b) Ellers kun oplysninger om: 1) Aktuel behandling 2) Om patienter i behandling på samme behandlingsenhed (organisatorisk tilknytning)	De oplysninger, som den sundhedsperson, sekretæren udfører teknisk bistand for, har adgang til	
Værdispringsreglen § 42 a, stk. 5[n]	Både oplysninger om aktuel og historisk behandling	Både oplysninger om aktuel og historisk behandling Adgangen er begrænset til egne systemer på behandlingsenheden	Ved teknisk bistand	***Patienten kan ikke sige fra***
Samtykkeregel § 42 a stk. 6	Både oplysninger om aktuel og historisk behandling	Oplysninger kan ikke indhentes	Ved teknisk bistand	***Patienten skal give samtykke***

[m] Ved et lukket system forstås et elektronisk system, der kun indeholder oplysninger til brug for behandling, som gives på det pågældende behandlingssted. Der er tale om et teknisk helt afgrænset system, hvorfra der ikke er direkte adgang til oplysninger fra andre, eksterne elektroniske patientsystemer, og hvortil der ikke kan indføres data fra andre eksterne elektroniske patientsystemer.

[n] Indhentning er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke kan varetage sine interesser, sundhedspersonen eller andre patienter.

2.3.3 Autorisationsloven og journalføringsreglerne

Informationssikkerhed har også en naturlig sammenhæng med reglerne om sundhedspersoners journalføring. Journalføringsreglerne er fastsat i autorisationsloven[3] samt de i medfør heraf udstedte administrative retsforskrifter[12]. Journalføringsreglerne er derfor inddraget i vejledningens beskrivelse af rettelser i patientjournaler, dokumentation af patienters samtykke og frabedelse af indhentning af oplysninger.

3 Konkret del

For det statslige områder er det obligatorisk at følge den danske standard for informationssikkerhed DS 484. Regeringen, Danske Regioner og KL skriver i den fællesoffentlige digitaliseringsstrategi[6], at standarden DS 484 skal udbredes til hele den offentlige sektor. Denne del af vejledningen er struktureret som DS 484. Standarden er generisk og forudsættes benyttet som grundlag for sundhedsvæsenets informationssikkerhed. Vejledningen supplerer og udfylder standarden på de punkter, hvor særlige forhold gør sig gældende i sundhedsvæsenet.

3.1 Risikovurdering og -håndtering

Formålet med risikovurderingen er at identificere risici med udgangspunkt i driftsmæssige forhold og danne grundlag for ledelsens beslutninger og prioriteringer af indsatsen mod risici.

3.1.1 Vurdering af sikkerhedsrisici

Gennemførelsen af systematisk risikoanalyse og – vurdering efter en valgt risikovurderingsmodel skal prioriteres højt, fordi resultaterne af risikovurderinger skal være sammenlignelige fra risikovurdering til risikovurdering. På denne måde kan ændringer i forhold til den foregående risikovurdering observeres og vurderes.

Risikovurderingen kan ske i to trin:

1. En overordnet vurdering af driftsmæssige risici, som ledelsen skal vurdere

2. For særlige kritiske driftsmæssige områder og aktiver skal der foretages en dyberegående risikovurdering af specifikke faglige kompetencer

3.1.2 Risikohåndtering

Risikohåndteringen betyder, at ledelsen prioriterer sikringsforanstaltninger til at reducere de identificerede risici til et acceptabelt niveau for ledelsen.

Ved risikovurdering skal man kortlægge mulige trusler. I sundhedsvæsenet er det især patientdata, som kan være værdifulde for eksterne parter.

I sundhedsvæsenet kan jagten efter ”den gode historie” fx om kendte personer og industrispionage være trusler.

Ofte er der tale om illegitim adgang til informationssystemer og data ved fx ”social engineering”, som er den mest almindelige metode, hvor en person i telefonen udgiver sig for at være en person fra fx en myndighed, en leverandør eller en it-medarbejder.

3.2 Overordnede retningslinier

Overordnede retningslinier refererer til ledelsens informationssikkerhedsstrategi, som indeholder en sikkerhedsmålsætning, som er besluttet ud fra en overordnet risikovurdering, en informationssikkerhedspolitik og en overordnet handlingsplan.

3.2.1 Informationssikkerhedsstrategi

Med hensyn til strategien er de primære opgaver følgende:

- Formulering af en informationssikkerhedspolitik
- Løbende vedligeholdelse af informationssikkerhedsstrategien

I informationssikkerhedspolitikken beskrives på et overordnet niveau de sikkerhedskrav, generelle krav til overholdelse af relevant lovgivning og kontraktlige forpligtelser, uddannelse og træning af medarbejdere, beredskabsplaner og konsekvenser ved overtrædelse af politikken. Desuden beskrives roller og ansvar ifm. informationssikkerheden og styringen af hændelser, som kan have indflydelse på informationssikkerheden.

It-strategien skal revurderes løbende som minimum en gang om året, og sundhedsvæsenet skal være opmærksom på, at revurderingen også skal ske i forhold til gældende lovgivning.

3.3 Organisering af informationssikkerhed

Formålet med organisering af informationssikkerhed er at styre organisationens informationssikkerhed internt og ved eksternt samarbejde.

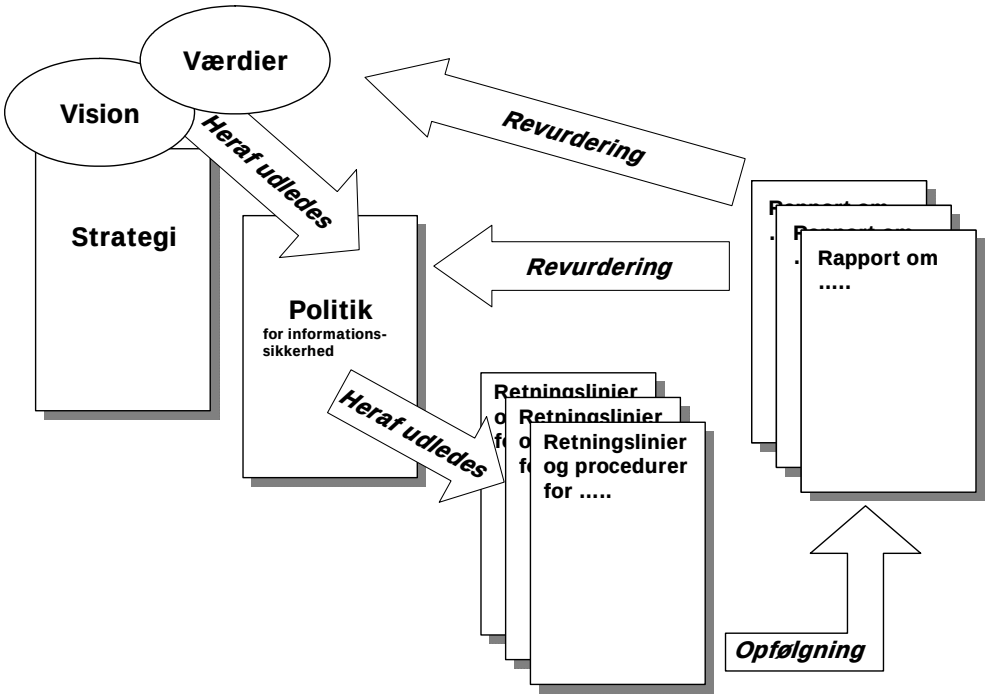
3.3.1 Interne organisatoriske forhold

For at sikre organiseringen af informationssikkerheden i organisationen skal ledelsen tage stilling til og beslutte sikringsforanstaltninger og implementeringsretningslinier set i forhold til følgende punkter:

- Ledelsens rolle
- Koordinering af informationssikkerhed
- Ansvarsplacering
- Godkendelsesprocedure ved anskaffelser
- Tavshedserklæringer
- Kontakt med myndigheder
- Fagligt samarbejde med grupper og organisationer
- Periodisk opfølgning

I større institutioner i sundhedsvæsenet er det formålstjenligt, at der etableres en formel informationssikkerhedsorganisation, der er forankret i den øverste ledelse. Desuden har informationssikkerhedsorganisationen brug for såvel sundhedsfaglig som it-faglig kompetence. Den bør ikke organisatorisk lægges under it- eller sundhedsfaglig ledelse, da der kan være situationer, hvor der kan være konflikt mellem faglige interesser og informationssikkerhedsmæssige interesser.

I små behandlingsenheder kan det være tilstrækkeligt, at ansvaret for opgaverne vedr. informationssikkerhed placeres entydigt.



Figur 1 Systematisk dokumentation vedr. informationssikkerhed

3.3.2 Eksterne samarbejdspartnere

Formålet med organisering af informationssikkerhed i forhold til eksterne samarbejdspartnere er at fastholde det vedtagne sikkerhedsniveau.

Ethvert formaliseret eksternt samarbejde skal være baseret på en samarbejdsaftale, som sikrer, at organisationens sikkerhedsmålsætning ikke kompromitteres. Der kan fx være tale om en leverandør af sundhedsfaglige ydelser (fx specialistundersøgelser eller -behandlinger) eller en leverandør af it-serviceydelser (fx netværk, serverhosting eller systemvedligeholdelse).

Alle sikkerhedsforhold skal være afklaret, før organisationens kunder eller eksterne interessenter får adgang til organisationens informationsbehandlingssystemer. Det kan fx dreje sig om on-line tidsbestilling eller receptfornyelse, eller der kan være tale om patienters adgang til at læse i EPJ.

3.4 Styring af informationsrelaterede aktiver

Formålet er at sikre og vedligeholde den nødvendige beskyttelse af organisationens informationsaktiver.

3.4.1 Identifikation af og ansvar for informationsrelaterede aktiver

Alle fysiske og funktionsmæssige informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig ejer. Med ejer menes i denne forbindelse en per-

son eller en organisatorisk enhed, som har fået tildelt det ledelsesmæssige ansvar for behandling, vedligeholdelse og anvendelse af samt adgang til et givet aktiv. En ejer har således ikke nødvendigvis noget juridisk ejerskab af aktivet[7].

Medarbejderne skal informeres om retningslinjerne for og sanktionerne ved misbrug eller manglende overholdelse heraf fx ved brug af e-mail, internet, brugen af mobilt udstyr fx bærbar computer, hvor medarbejderne transporterer og behandler patientdata internt eller eksternt.

3.4.2 Klassifikation af informationer og data

Formålet med klassifikation af informationer og data er at finde et passende beskyttelsesniveau for informationsaktiver, som indeholder informationer og data.

I sundhedsvæsenet bliver der arbejdet med patientdata indeholdende helbredsoplysninger, som er underlagt nogle lovmæssige krav. Det betyder, at informationer og data skal klassificeres på grundlag af deres driftmæssige værdi og lovmæssige krav.

Persondatalovens kapital 11 om behandlingssikkerhed stiller blandt andet krav om, at der træffes foranstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Der stilles således krav om integritet og fortrolighed.

For hvert klassifikationsniveau skal der være retningslinjer for behandling, lagring, transmission og destruktion samt logning, der er relateret til særligt klassificerede data.

3.5 Medarbejdersikkerhed

Med medarbejdersikkerhed forstås informationssikkerhedsemner, der relaterer sig til medarbejdere før, under og efter en ansættelse i sundhedsvæsenet.

Procedurer og kriterier, som måtte høre under medarbejdersikkerhed, beskrives for derved at opnå ensartet behandling af ansøgere ved ansættelsen, men også under ansættelsen og efter ansættelsen for at opnå et standardiseret sikkerhedsniveau.

Ledelsen har ansvar for at iværksætte, opretholde og vedligeholde sikringsforanstaltningerne i forhold til medarbejdersikkerhed.

3.5.1 Sikkerhedsprocedure før ansættelse

En sikkerhedsprocedure i form af ansættelsesprocedure skal indeholde følgende:

- opgaver og ansvar
- efterprøvning
- aftale om ansættelse

Ledelsen skal tage stilling til særlige roller og ansvar i forhold til informationssikkerhed i forbindelse med brugen af elektroniske systemer med patientdata i sundhedsvæsenet.

Det skal munde ud i sikringsforanstaltninger som at beskrive disse særlige roller og ansvar i stillings- og funktionsbeskrivelser inkl. vilkår i ansættelseskontrakten.

Desuden kan det inkorporeres i ansættelsesproceduren at tjekke identitet, CV, eksamenspapirer, referencer osv. og hvis nødvendigt at stille krav om kopi af straffeattest.

Sikringsforanstaltninger er nødvendige for såvel faste som midlertidige medarbejdere.

3.5.2 Ansættelsesforholdet

I ansættelsestiden er det nødvendigt at sikre det fornødne awareness- og uddannelsesniveau i organisationen, ligesom disciplinære foranstaltninger skal være tydelige for at signalere vigtigheden i overholdelsen af retningslinjerne, og nøgleordene er følgende:

- ledelsens ansvar
- uddannelse, træning og oplysning om informationssikkerhed
- sanktioner

Ledelsen på sygehusene, klinikkerne m.v. skal fx udarbejde instrukser til medarbejderne om betydningen af de nye regler om sundhedspersoners juridiske og tekniske adgang til elektroniske patientjournalsystemer og fx informere om den nye skærpede straffebestemmelse i sundhedslovens § 271, der hjemler bødestraf eller fængsel indtil 4 måneder.

Der skal føres tilsyn med, om instrukserne bliver fulgt.

3.5.3 Ansættelsens ophør

Ved ansættelsens ophør er det ligeledes vigtigt, at der er en klar procedure for, hvad medarbejderen skal gøre.

En medarbejder, der forlader organisationen, har stadig tavshedspligt med hensyn til de fortrolige data, vedkommende har haft kendskab til via sin stilling i ansættelsesperioden.

Der skal returneres organisationsaktiver som dokumenter, udstyr, adgangskort og kreditkort m.m.. Forskellige adgange og rettigheder skal inddrages. Endvidere bør leverandører, eksterne og interne samarbejdspartnere informeres om medarbejderens fratrædelse, for at der kan tages de fornødne sikringsforanstaltninger - fx kan der være tale om, at informationer tilflyder en fratrådt medarbejder, eller gruppeadgang, som medarbejderen har været en del af, og disse skal ændres.

3.6 Fysisk sikkerhed

Sikringsområdet fysisk sikkerhed består af to hoveddiscipliner: Sikre områder og beskyttelse af udstyr.

Formålet med sikringsforanstaltningerne i forhold til fysisk sikkerhed er at beskytte sundhedsvæsenets lokaler og informationsaktiver, f.eks. EPJ-systemer, mod uautoriseret fysisk adgang samt fysiske skader og andre forstyrrelser. Særligt kritisk informationsbehandlingsudstyr og tilhørende lagringsmedier skal placeres i sikre områder og beskyttes af de nødvendige fysiske barrierer og adgangskontroller. De fysiske beskyttelsesforanstaltninger skal afpasses efter de risici, der gør sig gældende inden for sundhedsvæsenet.

3.6.1 Sikre områder

Alt afhængig af hvilken del af sundhedsvæsenet der er tale om, vil der være forskellige risici i forhold til den fysiske sikkerhed. Derfor er der også forskel på kravene til den fysiske afgræsning.

En mindre klinik vil typisk have færre kontorer og lokaler og mindre udstyr end et hospital. På den anden side vil klinikken typisk ikke være bemandet om natten, som fx hospitalet. Denne forskel betyder, at implementeringen af sikringsforanstaltningerne skal angribes på forskellig vis på henholdsvis klinikken og hospitalet.

Afpasset forskellige driftsmæssige risici opbevares informationsaktiverne i forskellige sikkerhedszoner, hvor sikringsforanstaltningerne i form af fysiske barrierer og adgangskontroller tilsvarende vil variere.

Ved tilrettelæggelsen af fysisk sikkerhed skal der tages hensyn til skadevirkninger fra omgivelserne som temperatur og fugtighed, nærliggende trafikanlæg, som kan give anledning til specielle sikkerhedstiltag og natur- eller menneskeskabte trusler som brand, oversvømmelser, civile optøjer osv. Inden for sundhedsvæsenet er det bl.a. relevant at tage hensyn til beskyttelse af elektronisk udstyr, fx overvågningsudstyr, på operations- og intensivafsnit mod varme- og fugtpåvirkninger samt forstyrrelse fra mobiltelefoner.

Arbejdsmæssige forhold i sikre områder skal beskrives, dvs. instrukser og procedurer.

Af- og pålæsningsområder samt andre områder, hvor offentligheden kan få adgang, skal være overvåget og følge lovgivningens krav.

Det er karakteristisk for sundhedsvæsenet, at der passerer mange mennesker gennem dets lokaler hver dag. Derfor er det relevant at overveje den fysiske sikring af særlige områder og placering af arbejdsstationer, hvorfra der er adgangsmulighed til personhenførbare informationer, jf. sikkerhedsvejledningen.

En fysisk sikring af informationsaktiver, f.eks. papirarkiv og it-ressourcer, herunder også netværk (kabler, stik, krydsfelter mv.) tager i første omgang sigte på en afgrænsning og tilstrækkelig overvågning af de geografiske og lokalemæssige forhold. Det drejer sig om hensyntagen til forhold, som kan have indflydelse på installationerne, både de nære som de fjerne, herunder sikring mod vand, brand og hærværk.

3.6.2 Beskyttelse af udstyr

Beskyttelse af udstyr dækker i hovedtræk følgende:

- Placering af udstyr
- Forsyningssikkerhed
- Sikring af kabler
- Udstyrs og anlægsvedligeholdelse
- Sikring af udstyr uden for organisationens overvågning
- Sikker bortskaffelse eller genbrug af udstyr
- Fjernelse af organisationens informationsaktiver

Det gælder om at minimere risikoen for tab, skader og uautoriseret dataadgang og i det hele taget at undgå forstyrrelser af informationsaktiver og patientsikkerheden i sundhedsvæsenet.

Udstyr deriblandt kabler skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyret skal vedligeholdes efter forskrifter.

Desuden skal udstyret sikres mod forsyningssvigt i overensstemmelse med dets betydning for kritiske driftssystemer. Ved bortskaffelse eller ved genbrug skal udstyret enten fysisk destrueres eller overskrives iht. en anerkendt metode.

3.7 Styring af netværk og drift

3.7.1 Operationelle procedurer og ansvarsområder

Formålet er at sikre stabil og betryggende drift.

Sikring af den daglige drift sker først og fremmest gennem fastlæggelsen af ansvar for styring og drift af organisationens informationsaktiver samt procedurebeskrivelser af de vigtigste driftsopgaver som driftsplanlægning, backup, fejlhåndtering, håndtering af særlig fortrolige data, retableringsprocedurer, software og hardware opdateringer og logninger.

Herudover skal ændringer til kritiske informationsaktiver håndteres ved en formaliseret procedure.

Proceduren skal omfatte dokumentation af ændringer, plan for testforløb, godkendelsesforløb for at sætte ændringer i produktion, dvs. i driftsmiljøet, advisering af interessenter, og plan for hvordan en ændring kan ”rulles tilbage”, hvis tingene ikke går efter planen.

Det er vigtigt, at der er adskillelse mellem udvikling, test og drift, for at sikre, at driftsmiljøet ikke bliver forstyrret af udvikling eller test.

3.7.2 Ekstern serviceleverandør

I forbindelse med implementering og opretholdelse af et ønsket sikkerhedsniveau kan organisationen indgå et samarbejde med en ekstern serviceleverandør. Der skal i så fald udpeges en ansvarlig kontakt både i organisationen og hos serviceleverandøren. Et sådant samarbejde ændrer dog ikke på, at det overordnede ansvar for informationssikkerheden påhviler organisationen.

3.7.3 Styring af driftsmiljøet

En styring af driftsmiljøet er medvirkende til at minimere risikoen for teknisk betingede nedbrud. Inden for sundhedsvæsenet er en vis grad af langtidsplanlægning påkrævet for at sikre tilstrækkeligt kapacitet. Dette gælder særligt i forhold til store behandlingsenheder, fx hospitaler.

Der skal i forlængelse af langtidsplanlægningen fortages en løbende kapacitetsfremskrivning baseret på de fremtidige forventninger og prognoser og de heraf afledte kapacitetskrav. Lovændringer kan medføre øgede krav til systemerne eller specifikke systemkrav.

3.7.4 Skadevoldende programmer og mobil kode

Et vigtigt element i opretholdelsen af informationssikkerhed er at beskytte organisationen mod skadevoldende programmer, fx virus, orme, trojanske heste og logiske bomber. Informationsbehandlingsprogrammer kan være sårbare over for angreb fra skadevoldende programmer. Derfor er det nødvendigt at træffe sikringsforanstaltninger for at forhindre og konstatere angreb af skadevoldende programmer. De ansatte i sundhedsvæsenet er med til at opretholde beskyttelsen af informationsbehandlingssystemerne ved at være opmærksomme på uregelmæssigheder i systemerne, fx at man har adgang til oplysninger, som man ikke er autoriseret til.

3.7.5 Sikkerhedskopiering

Informationsaktiverne i sundhedsvæsenet indeholder mange data, som er værdifulde for de ansatte i sundhedsvæsenet, da de er afhængige af informationerne for at kunne udføre deres arbejdsopgaver. Patientjournalerne fungerer som et arbejdsredskab for sundhedspersonalet. De lagrede data er endvidere betydningsfulde for patienterne, fx i forbindelse med aktindsigt. Som et led i at sikre den ønskede tilgængelighed til informationsaktiverne, skal der foretages sikkerhedskopiering. Kopieringen skal foregå efter faste procedurer. Der skal ske en løbende afprøvning af kopiernes anvendelighed.

I nogle tilfælde kan det være uforholdsmæssigt vanskeligt (i forhold til konsekvenserne af datatab og mulighederne for at genskabe data), at foretage en sikkerhedskopiering. Det kan fx dreje sig om sikkerhedskopiering af data fra visse typer af medicoteknisk udstyr. Med baggrund i en risikovurdering kan ledelsen derfor i særlige tilfælde vælge at undlade at foretage en sikkerhedskopiering.

3.7.6 Netværkssikkerhed

Formålet med sikringsområdet netsværkssikkerhed er at beskytte transmitterede data og den underliggende infrastruktur.

Ved transmission af fortrolige oplysninger over åbne net (fx internet), herunder personnummer, skal der som minimum foretages kryptering. Hvis de transmitterede oplysninger er af følsom karakter, herunder helbredsoplysninger, skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.

3.7.7 Databærende medier

Databærende medier skal beskyttes og deres distribution skal styres i overensstemmelse med de lagrede datas klassifikation.

Der skal foreligge instrukser for modtagelse, registrering, behandling, opbevaring, forsendelse og sletning af oplysninger fra bærbare datamedier som eksempelvis papir, magnetbånd, disketter, flytbare diske, mobile lagringsenheder og CD-rom'er.

Medicoteknisk udstyr, der indeholder personhenførbare informationer, ekkokardiografer, CT- og MR-scannere, monitoreringsudstyr og lignende, er omfattet af persondataloven. I sådant udstyr er der oftest tale om såkaldt 'kortvarig lagring' af oplysninger – en midlertidig lagring, der mister sin aktualitet, når fx undersøgelsessvar er afsendt eller den pågældende patient ikke længere har behov for udstyret. I sådanne situationer skal data slettes, når de ikke længere skal anvendes til de formål, som databehandlingen varetager, eller til kontrol med de inddaterede personoplysninger er uaktuel, dog senest efter en af den dataansvarlige nærmere fastsat frist[o].

3.7.8 Informationsudveksling

Formålet med sikringsforanstaltninger i forbindelse med informationsudveksling er at fastholde informationssikkerheden under forsendelse, transmission og anden udveksling af information både internt og eksternt.

Udveksling af information skal være baseret på faste retningslinjer, og der skal være procedurer, informationsudvekslingsaftaler og regler for beskyttelse af information under forsendelse, transmission og anden udveksling.

Elektroniske meddelelser i form af elektronisk post, dokumentudveksling, fildeling og lignende kommunikationsformer skal beskyttes.

Udveksling af personhenførbare informationer over åbne net, fx internettet, skal ske ved anvendelse af stærk kryptering[10] [11].jf. pkt. 3.9.3. Både afsenders og modtagers autenticitet skal sikres, og dette skal i sundhedsvæsenet ske ved anvendelse af offentlig digital signatur[13] (OCES). Der skal foreligge aftaler om informationsudveksling, hvad enten udvekslingen sker fysisk eller elektronisk. Aftalens sikringsforanstaltninger skal være i overensstemmelse med klassifikationen af de informationer, der udveksles.

---

[o] Sikkerhedsbekendtgørelsens § 10, stk. 2, og § 13, stk. 4

3.7.9 Elektroniske forretningsydelser

Informationer i forbindelse med offentlige elektroniske serviceydelser skal beskyttes mod uautoriseret adgang og ændringer.

I sundhedsvæsenet kan ydelserne fx dreje sig om patienters adgang til receptfornyelse, booking, e-mail-konsultation eller mulighed for attestudstedelse på basis af eksisterende patientjournaldata.

I situationer, hvor patienter tilbydes mulighed for via internettet eller sundhed.dk at skrive i deres egen EPJ, skal der indføres særlige sikringsforanstaltninger for at forhindre transmissionsfejl, fejladressering, manipulation samt uautoriseret adgang og retransmission.

3.7.10 Logning og overvågning

Formålet med logning og overvågning er at afsløre uautoriserede handlinger. Informationsbehandlingssystemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres. Der skal være logning, som sikrer, at uønskede forhold konstateres. Ligeledes skal der være en overvågning, som skal verificere, at sikringsforanstaltningerne fungerer efter hensigten.

Denne del af sikringsområdet styring af netværk og drift er særligt relevant for sundhedsvæsenet pga. lovgivningens krav til logning og udviklingen af et mere gennemsigtigt sundhedsvæsen med øgede patientrettigheder. Et eksempel herpå er, at de registrerede (patienterne) i Medicinprofilen og patienter, der har en digital signatur via sundhed.dk har adgang til logoplysninger fra Medicinprofilen og opslag i Landspatientregisteret.

I persondataloven er der fastsat regler om behandlingssikkerhed, som har betydning for organisationens logning og overvågning. Efter persondatalovens § 41, stk. 3, er det et krav, at den dataansvarlige træffer de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Det samme gør sig gældende for databehandlere.

Efter persondatalovens § 41, stk. 5, kan justitsministeren fastsætte nærmere regler om sikkerhedsforanstaltninger. I sikkerhedsbekendtgørelsens § 19 er der fastsat nærmere krav om logning.

Kravet om logning har navnlig til formål at sikre et revisionsspor, således at det efterfølgende kan klarlægges, hvilken bruger der har foretaget en bestemt anvendelse af et system, fx har søgt bestemte oplysninger om en bestemt person. Logning har af denne grund også et præventivt sigte. Logningen skal bl.a. omfatte en angivelse af den patient, som de anvendte oplysninger vedrørte eller det angivne søgekriterium[10].

Logningens omfang

Alle brugeraktiviteter, afvigelser og sikkerhedshændelser skal logges og opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.

Adgang til patientoplysninger ved brug af den særlige autorisering i forbindelse med værdispringsreglen skal fremgå af loggen.

Det følger af sikkerhedsbekendtgørelsens § 19, stk. 1, at der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Sikkerhedsbekendtgørelsens § 19, stk. 2-5, indeholder undtagelser til kravet om logning. Af særligt relevans for sundhedsvæsenet er § 19, stk. 4, hvorefter der ikke skal logges, hvis behandlingen af personoplysningerne udelukkende sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med et kodenummer eller lignende. Der skal dog foretages maskinel logning af bruger og tidspunkt for behandlingen.

For så vidt angår undtagelser fra kravet om logning er det endvidere vigtigt at være opmærksom på sikkerhedsbekendtgørelsens § 19, stk. 5. Bestemmelsen fastslår, at der ikke er et krav om logning i forbindelse med behandling af personoplysninger, som i form af måle- eller analyseresultater automatisk lagres i medicoteknisk udstyr. Undtagelsen omfatter tillige personoplysninger, som manuelt registreres i medicoteknisk udstyr til supplering af automatisk lagrede oplysninger. Eksempler på relevant udstyr i denne forbindelse er mobile eller bærbare blodtryksmonitorer og blodsukkermåleapparater.

Datatilsynet kan i forbindelse med en godkendelse af en anmeldelse stille krav om specifikke efterfølgende kontrolforanstaltninger som et vilkår for godkendelsen.

For så vidt angår eksempler på efterfølgende kontrolforanstaltninger er Datatilsynets udtalelse af 22. september 2006 vedr. privatpraktiserende lægers adgang til e-journal illustrativ. Af udtalelsen fremgår det, at de privatpraktiserendes lægers adgang til e-journal skal følges op af en række efterfølgende kontrolforanstaltninger. Kontrolforanstaltningerne består af fremsendelse af månedlige opgørelser til de deltagende amters (regioners) administratorer over alle sygehus- og sundhed.dk-brugere, der viser antal foretagne logins, antal afgivne samtykker på specifikke personnumre samt antal skift fra egen amtsserver til anden amtsserver. Endvidere skal borgere orienteres pr. sikker e-post eller brev, når en læge i e-journal har gjort sig bekendt med oplysninger om en person, der ikke er tilknyttet lægens ydernummer. Desuden skal der som minimum gennemføres kontrol af 1 % af alle 'normale' opslag og kontrol af 10 % af alle 'akut ekstraordinære opslag'

Patienters adgang til logoplysninger (sundhedslovens § 42 c)

Efter den gældende lovgivning har patienter ikke et retskrav på, at få adgang til logoplysninger. Dette skyldes, at offentlige dataansvarlige efter de gældende regler ikke har pligt til at give registrerede elektronisk adgang til oplysninger i loggen.

Indenrigs- og sundhedsministeren har efter sundhedslovens § 42 c fået bemyndigelse til at fastsætte nærmere regler om patientens elektroniske adgang til oplysninger hos offentlige og private dataansvarlige om, hvem der har foretaget opslag i patientens elektroniske patientjournal, og på hvilket tidspunkt opslagene er foretaget. Det fremgår af bemærkningerne til bestemmelsen, at bemyndigelsen vil blive udnyttet, når der er teknisk mulighed herfor uden uforholdsmæssige omkostninger

for de dataansvarlige og at det indebærer, at bemyndigelsen således først vil blive udnyttet, når det systemteknisk er muligt elektronisk at generere og udskrive de pågældende oplysninger på en måde, så oplysningerne uden væsentlig efterfølgende administrativ sagsbehandling kan læses og forstås af patienten og uden uforholdsmæssige omkostninger for de enkelte dataansvarlige. Det er således en forudsætning, at oplysningerne gives til patienten på en for denne let forståelig måde.

Den nationale IT-strategi for sundhedsvæsenet vil kunne bidrage til at skabe klarhed over, hvornår der realistisk kan forventes at være implementeret sådanne løsninger – i både eksisterende og kommende it-systemer – som muliggør, at patienter sikres adgang til log-oplysninger i en form, som er let forståelig for patienten og uden uforholdsmæssige omkostninger for de enkelte dataansvarlige.

Det fremgår endvidere af bemærkningerne til bestemmelsen i § 42 c, at bemyndigelsen til at fastsætte regler om patienters adgang til log-oplysninger vil blive udnyttet, når der foreligger tilstrækkelig klarhed omkring disse forhold, at det vil blive tilstræbt, at en sådan klarhed foreligger senest ultimo 2008, og at det således vil være muligt at fastsætte regler om patienters adgang til log-oplysninger senest den 1. januar 2009.

Frem til udnyttelse af bemyndigelsen har patienter således ikke krav på indsigt i logoplysninger om, hvem der har foretaget opslag i patientens elektroniske patientjournal, og på hvilket tidspunkt opslagene er foretaget, men hvis der systemteknisk er mulighed herfor, kan en sådan adgang naturligvis etableres af den dataansvarlige.

Patienters adgang til logoplysninger bør derfor indtænkes i de nye tekniske systemer.

Alle afviste adgangsforsøg skal registreres. Afviste adgangsforsøg anses for uregelmæssigheder, der skal analyseres og følges op efter nærmere fastsat instruks[9].

Der skal tages de nødvendige forholdsregler for at beskytte loggen mod illegitim adgang og mod sletning. Loggen skal opbevares i 6 måneder og derefter slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år[9].

3.8 Adgangsstyring

3.8.1 De forretningsmæssige krav til adgangsstyring

Formålet med adgangsstyring er at styre adgangen til organisationens systemer, informationer og netværk med udgangspunkt i de virksomhedsmæssige og lovgivningsbetingede krav.

Inden for sundhedsvæsenet er der mange forskelligartede behandlingsenheder både i relation til sammensætning af personale, størrelse og arbejdsområde. Det er op til den enkelte behandlingsenhed, hvordan sikringsforanstaltningerne implementeres, så længe det sker inden for lovens rammer. Der skal foreligge dokumenterede og ajourførte retningslinjer for styring af såvel logisk som fysisk adgang til informationsaktiver.

En af måderne, til at kunne styre adgangen til systemerne, informationerne og netværkene på, er at udarbejde dokumenterede og ajourførte retningslinier for adgangsstyringen. Retningslinierne for adgangsstyring skal fastlægge adgangsregler og -rettigheder.

En vigtig del af adgangsstyringen er administration af brugeradgang, herunder registrering af brugere og muligheden for at tildele og anvende udvidede adgangsrettigheder. I forlængelse heraf spiller tildelingen af adgangskoder en vigtig rolle. En sådan tildeling sker ved en formaliseret proces, og der sker en periodisk gennemgang af brugernes rettigheder.

3.8.2 Administration af brugeradgang

Der skal være en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang.

Principperne for autorisering til brugeradgang er:

- Autorisering gives alene til data og funktioner, der er nødvendige for at varetage personens arbejdsopgaver
- Autorisering gives alene for perioder, hvor personen arbejdsmæssigt er tilknyttet den pågældende behandlingsenhed (fx klinik, skadestue, ambulatorium eller hospital). Autorisering er en formel procedure, hvorved adgangstilladelse besluttes. Dette bør ske på et organisatorisk niveau, der er umiddelbart foresat den ansatte (’nærmeste leder’) og i nært samarbejde med organisationens personalefunktion. På basis af autoriseringen tildeles adgangsrettigheder. Tilsvarende bør tilbagekaldelse af autoriseringen nøje afspejle omplaceringer, længerevarende fravær og fratræden. Også i disse situationer bør der være et nært samarbejde mellem relevante ledelsesniveauer og personalefunktion.

Brugeres autorisation til data og funktionaliteter gennemgås periodisk efter instruks herom.

Autoriseringens omfang

For at regulere adgangen til helbredsoplysninger i elektroniske systemer i forbindelse med aktuel behandling af patienter iht. kravene i lovgivningen, skal systemernes adgangskontrol som nævnt baseres på den enkelte medarbejders autorisering til behandling af data i forbindelse med den enkelte ansattes udførsel af vedkommendes arbejdsopgaver.

Det afhænger af medarbejderes rolle og tilknytning til en bestemt del af organisationen, hvilken information, medarbejderne kan autoriseres til at få adgang til. Den enkelte medarbejder må kun autoriseres til at få adgang til oplysninger i de elektroniske systemer, som medarbejderen har en organisatorisk tilknytning til. I relation til EPJ-systemer er det kun sundhedspersoner, der har et sagligt behov for at få adgang til EPJ-systemer, der må autoriseres hertil, og den enkelte sundhedsperson må alene autoriseres til anvendelser (dvs. få teknisk adgang til oplysninger), som vedkommende har behov for.

Sundhedslovens indhentningsregler fastlægger rammerne for, hvilke oplysninger en sundhedsperson i forbindelse med aktuel behandling af patienter må autoriseres

til anvendelse af. I vejledningens generelle del er de generelle og konkrete adgangsbetingelser efter sundhedsloven behandlet. I nærværende sammenhæng fremhæves de dele af bestemmelserne, som er særlig relevante i forhold til adgangsstyring.

Sundhedslovens regler om indhentning af elektroniske helbredsoplysninger bygger grundlæggende på, at der skal være etableret en patient-behandler-relation for, at det er tilladt, at en sundhedsperson indhenter patientdata. Loven giver en differentieret adgang til EPJ-systemer, som understøtter det behov de pågældende sundhedsfaglige grupper har for at få adgang til oplysningerne pga. deres arbejdsopgaver. Alle sundhedspersoner kan få adgang til at indhente helbredsoplysninger m.v. fra EPJ-systemer til brug for aktuel patientbehandling.

Efter sundhedslovens indhentningsregler sondres mellem følgende faggrupper:

- Læger, sygehusansatte tandlæger og medicinstuderende
- Andre sundhedspersoner
- Andre sundhedspersoner med udvidet adgang (tilladelse fra ledelsen)
- Sekretærer

Læger, sygehusansatte tandlæger og medicinstuderende under ansvar af en læge eller en sygehusansat tandlæge får en bred adgang til EPJ-systemer. Dvs., en adgang til at indhente historiske og aktuelle patientdata og efter omstændighederne adgang til at søge på tværs af organisatoriske grænser og sektorer i den udstrækning, systemerne teknisk giver mulighed herfor. De persondataretlige sikkerhedsregler bl.a. vedr. autorisationer skal iagttages i denne sammenhæng.

Gruppen af andre sundhedspersoner end læger, sygehusansatte tandlæger og medicinstuderende får adgang til at indhente aktuelle helbredsoplysninger fra EPJ-systemer for de patienter, som er tilknyttet samme behandlingsenhed som sundhedspersonen. Kravet om tilknytning til samme behandlingsenhed indebærer et krav om, at sundhedspersonen og patienten er tilknyttet samme behandlingsenhed, hvor der udføres sundhedsfaglig virksomhed. Denne tilknytning skal afspejles i den pågældende sundhedspersons systemtekniske adgang. Ved udtrykket behandlingsenhed forstås sygehus, sygehusafdeling, afsnit, klinik eller lign., idet kravet om organisatorisk tilknytning datasikkerhedsmæssigt skal administreres så snævert, som det teknisk er muligt. Sundhedsloven stiller således krav om, at andre sundhedspersoner end læger, sygehusansatte tandlæger og medicinstuderende ikke må få adgang til patienter, der ikke er tilknyttet samme behandlingsenhed som sundhedspersonen.

Det er også centralt for adgangsstyringen til EPJ-systemer, at andre sundhedspersoner end læger, sygehusansatte tandlæger og medicinstuderende som udgangspunkt kun får adgang til at indhente oplysninger om aktuel behandling. Ved oplysninger om aktuel behandling forstås, jf. pkt. 2.3.2.3, som udgangspunkt oplysninger registreret eller indhentet efter en bestemt dato, fx indlæggelsesdatoen eller datoen for iværksættelsen af et ambulant forløb. Ved genindlæggelser inden for en kortere periode for samme helbredsproblem, hvor indlæggelserne må betragtes som en del af et sammenhængende behandlingsforløb, vil oplysninger om de tidligere indlæggelser ligeledes være oplysninger om aktuel behandling. En sundhedsperson,

der foretager opslag i elektroniske systemer, må således foretage en vurdering af, om de elektroniske helbredsoplysninger, der søges indhentet, vil være oplysninger om aktuel behandling.

Oplysninger, som efter indlæggelsen på behandlingsstedet er registreret eller indhentet på en anden afdeling eller et andet afsnit om den aktuelle behandling på behandlingsstedet, vil også være omfattet af begrebet aktuelle oplysninger. Dvs. at en sundhedsperson, der arbejder på et kirurgisk sengeafsnit, efter bestemmelsen vil have adgang til de aktuelle oplysninger, der er registreret om patienten på operations- og anæstesiafdelingen, til brug for sundhedspersonens aktuelle behandling. Sundhedspersoner på et sygehus har således adgang til de nødvendige aktuelle data om en patient, hvis der er behov herfor i forbindelse med behandling af en patient.

Den sundhedsperson, der er ansvarlig for behandlingen af en patient, har efter omstændighederne adgang til at aktualisere helbredsoplysninger, der vedrører en tidligere behandling af patienten. Dvs., at sundhedspersonen ved fx at kopiere oplysninger over i et EPJ-modul med aktuel status, gør oplysninger fra tidligere behandlingsforløb tilgængelige for de sundhedspersoner, der er involveret i den aktuelle behandling af patienten. Dette kræver, at sundhedspersonen har en autorisation, der giver adgang til at foretage opslag på historiske oplysninger, og at sundhedspersonen vurderer, at det vil være relevant for de sundhedspersoner, der medvirker til behandlingen af patienten at kende oplysningen for at give patienten en effektiv behandling af høj kvalitet.

Begrebet 'oplysninger om aktuel behandling' skal ikke forstås snævert, således at oplysningerne kun stammer fra den igangværende indlæggelse.

Begrebet 'oplysninger om aktuel behandling' udelukker ikke, at der kan være tale om oplysninger, der oprindeligt er journalført i forbindelse med en tidligere indlæggelse, men nu bliver aktuelle igen til brug for den igangværende behandling. Har en patient fx for år tilbage gennemgået en behandling for samme sygdom som patienten aktuelt bliver behandlet for, vil det efter omstændighederne være nødvendigt at indhente de tidligere journalførte oplysninger og på denne måde gøre oplysningerne tilgængelige for de relevante sundhedspersoner, der alene har adgang til oplysninger om aktuel behandling. Det bemærkes, at det kun er sundhedspersoner med en adgang til historiske oplysninger, der kan indhente sådanne oplysninger og gøre dem tilgængelige for de øvrige sundhedspersoner, der er involveret i behandlingen af patienten.

Begrænsningen indebærer, at sundhedsloven stiller krav om, at gruppen af andre sundhedspersoners adgangsrettigheder datasikkerhedsmæssigt så vidt muligt skal administreres med henblik på at sikre, at historiske oplysninger er teknisk utilgængelige for de pågældende.

Som anført under den generelle del af vejledningen gælder de almindelige videregivelsesregler i sundhedsloven ved siden af indhentningsreglerne. Det betyder, at hvis en sundhedsperson er afskåret fra elektronisk at indhente historiske oplysninger efter § 42 a, stk. 2, vil videregivelsesreglerne efter omstændighederne kunne anvendes. Det betyder, at opstår der en situation, hvor fx en social- og sundhedsassistent har behov for yderligere oplysninger vedr. en patients tidligere indlæggelsesforløb, men social- og sundhedsassistenten ikke selv har adgang til oplysningerne, må social- og sundhedsassistenten få videregivet oplysningerne manuelt fra en sundhedsperson med bred adgang til EPJ-systemerne.

Efter sundhedslovens § 42 a, stk. 4, kan andre sundhedspersoner, når ledelsen på det behandlingssted, hvor den pågældende er ansat, har givet tilladelse hertil opgraderes til at få samme adgang til EPJ som læger, sygehusansatte tandlæger og medicinstuderende.

En sådan tilladelse indebærer, at de nævnte sundhedspersoner får samme adgang til at indhente oplysninger fra elektroniske systemer som læger og sygehusansatte tandlæger og dermed i modsætning til de øvrige sundhedspersoner får adgang til at indhente navnlig historiske data og efter omstændighederne adgang til at søge på tværs af organisatoriske grænser og sektorer i den udstrækning, systemerne teknisk giver mulighed herfor.

En tilladelse kan gives til enkelte navngivne sundhedspersoner, eller den kan være rettet mod en gruppe af sundhedspersoner, der fx varetager en bestemt funktion. Beslutninger om sådanne tilladelser skal fremgå af datasikkerhedsinstruksen for behandlingsstedet.

Det er et krav efter sundhedsloven, at beslutninger om tilladelser til, at andre sundhedspersoner end læger og sygehusansatte tandlæger kan indhente elektroniske helbredsoplysninger m.v. i udvidet omfang - navnlig historiske data og efter omstændighederne adgang til at søge på tværs af organisatoriske grænser og sektorer i den udstrækning, systemerne teknisk giver mulighed herfor - skal gøres offentligt tilgængelige.

Sikkerhedsmæssige hensyn kan i denne forbindelse tale for at klassificere dele af en datasikkerhedsinstruks som ikke offentligt tilgængelig, hvorfor der ikke efter sundhedsloven stilles krav om, at hele instruksen skal gøres offentlig tilgængelig. Der stilles endvidere ikke krav om en bestemt offentliggørelsesform. Offentliggørelse vil bl.a. kunne ske på behandlingsstedets hjemmeside.

Sekretærer får efter sundhedsloven under en sundhedspersons ansvar adgang til at yde teknisk bistand til opslag i EPJ. En sekretær kan yde teknisk bistand til opslag og indtastning af oplysninger efter en konkret anmodning eller efter en generel aftale med den ansvarlige sundhedsperson herom. Sekretærens adgang til at foretage opslag og indtaste oplysninger i de elektroniske systemer afhænger således af, hvordan arbejdsprocedurerne konkret er tilrettelagt på det enkelte behandlingssted, og hvilke opgaver sekretæren i den forbindelse er ansat til at udføre under ansvar af de relevante sundhedspersoner. Det vil således være omfattet af sundhedslovens adgang til at yde teknisk bistand, hvis en sekretær fx efter generel aftale med en læge eller sygeplejerske aftaler tid med patienter for nærmere bestemte undersøgelser og behandlinger, fører temperaturkurver og medicinkort, indhenter laboratoriesvar, afgiver prøvesvar til patienter osv., og i forbindelse med udførelsen af disse opgaver fører de relevante oplysninger ind i de elektroniske patientjournaler.

Lukkede systemer (sundhedslovens § 42 a, stk. 3)

Sundhedslovens § 42 a, stk. 3, tager højde for den særlige problemstilling, som knytter sig til visse steder uden for sygehusvæsenet, hvor der føres sundhedsfaglige optegnelser i egne, afgrænsede elektroniske systemer, og hvor der ikke er en læge eller en sygehusansat tandlæge involveret i behandlingen eller plejen. Det kan fx være hos en psykolog, kiropraktor, privatpraktiserende tandlæge, fodterapeut el. lign. eller i forbindelse med plejehjemsvirksomhed eller hjemmepleje, der indebærer sundhedsfaglige optegnelser.

I sådanne tilfælde vil der være behov for, at de ansatte sundhedspersoner kan få adgang til såvel oplysninger om aktuel behandling som historiske data. Derfor har andre sundhedspersoner end læger eller sygehusansatte tandlæger på det pågældende behandlingssted fået juridisk adgang til at foretage opslag i både historiske og aktuelle patientdata. Det gælder dog ikke, hvis der er en læge eller en sygehusansat tandlæge ansat på det pågældende behandlingssted, idet denne i givet fald vil kunne foretage de nødvendige opslag og i fornødent omfang videregive oplysningerne efter de almindelige videregivelsesregler.

Bestemmelsen om lukkede systemer tager således sigte på mindre behandlingssteder, fx en kiropraktor- eller en fodterapeutklinik, hvor patientdata føres i et system, som kun anvendes af personalet på det pågældende behandlingssted.

Ved behandlingssted forstås en myndighed, institution, virksomhed m.v. med egen ledelse, hvor der udføres sundhedsfaglig behandling, jf. sundhedslovens § 5, og foretages sundhedsfaglige optegnelser i egne, afgrænsede elektroniske systemer., Bestemmelsen stiller ikke krav om, at behandlingsstedet fysisk er samlet ét bestemt sted. Behandlingssteder, der udfører behandling flere forskellige steder decentralt, kan således betragtes som ét behandlingssted, f.eks. den kommunale hjemmesygepleje, der kan udføre behandling i patientens eget hjem, på institution eller i et eventuelt sundhedscenter, eller den kommunale skoletandpleje, der udfører tandbehandling på de enkelte skoler i kommunen. Det er dog som nævnt en forudsætning efter bestemmelsen, at de helbredsoplysninger, der er indeholdt i behandlingsstedets elektroniske systemer, alene er oplysninger til brug for behandling, som gives på det pågældende behandlingssted.

Begrebet ‘lukket system’ skal ikke forstås som et system med en fysisk afgrænsning, men derimod som en logisk afgrænsning. Et EPJ-system, som deler patientdata mellem to behandlingssteder er ikke et ‘lukket system’, da personalet på to behandlingssteder har adgang til oplysningerne i EPJ-systemet.

Eksempelvis vil et behandlingssted med et elektronisk patientjournalsystem, der har etableret en gensidig VPN (Virtual Private Network)-adgang til det regionale hospitals patientjournalsystem ikke have karakter af et ‘lukket system’, da behandlingsstedet og regionshospitalet via VPN-adgangen kan importere og eksportere indhente data mellem systemerne.

Det afgørende er, om de ansatte på det pågældende behandlingssted ved opslag i systemet alene kan indhente oplysninger til brug for behandling på det pågældende behandlingssted. I så fald er der tale om et ’lukket’ system efter sundhedsloven.

Det er endvidere afgørende, om andre end de ansatte på behandlingsstedet kan få elektronisk adgang til de helbredsoplysninger, der er lagret i behandlingsstedets selvstændige system. Har andre end de ansatte en sådan adgang, vil systemet ikke være et ‘lukket system’ i § 42 a, stk. 3’s forstand.

Langt de fleste behandlingssteder benytter sig af elektronisk overførsel af recepter via åben datakommunikation. Den gældende standard LMS016, som afløser EDIFACT-meddelelser, benyttes af de fleste praktiserende læger. Uanset et behandlingssted benytter sig af elektronisk udstedelse og videresendelse af recepter til apoteker, vil behandlingsstedets system ikke på grund af dette miste sin karakter af at være et lukket system i § 42 a, stk. 3’s forstand.

Behandlingssteder med et selvstændigt elektronisk patientjournalsystem, der kun indeholder helbredsoplysninger om de patienter, der har været indlagt på eller tilknyttet til behandlingsstedet, og hvor kun personalet på behandlingsstedet har adgang til systemer, er et 'lukket system'.

Værdispringsreglen (sundhedslovens § 42 a, stk. 5)

Sundhedspersoner kan efter sundhedsloven foretage opslag på helbredsoplysninger m.v., hvis det er nødvendigt til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, sundhedspersonen eller andre (værdispringsregel).

Reglerne tager højde for de situationer, hvor der opstår et øjeblikkeligt behandlingsbehov og der som følge heraf er brug for, at sundhedspersoner kan indhente helbredsoplysninger m.v. fra EPJ-systemerne om en patient meget hurtigt for at kunne behandle patienten.

Sundhedslovens værdispringsregel regulerer ikke alene situationer, hvor der opstår et øjeblikkeligt behandlingsbehov, men ligeledes situationer, hvor tungtvejende hensyn til patienten, sundhedspersonen eller andre legitimerer et opslag i EPJ-systemerne uden patientens samtykke, og hvor patienten ikke kan frabede sig opslaget.

Værdispringsreglen kan fx være relevant i situationer, hvor en person er blevet udsat for smitte (fx ved at have fået en stikskade) fra en person, som formodes at have smitsom leverbetændelse eller anden alvorlig smitsom sygdom, eller på anden måde er blevet særlig udsat for smitte. Hvis indhentningen af helbredsoplysninger m.v. om den smittebærende person er nødvendig med henblik på behandling af den smittede, og den smittebærende person ikke giver samtykke eller ikke umiddelbart kan findes, kan der ske indhentning efter værdispringsreglen.

Alle sundhedspersoner kan foretage opslag efter værdispringsreglen. Læger, sygehusansatte tandlæger, medicinstuderende og sundhedspersoner med tilladelse til udvidet adgang kan foretage opslag efter værdispringsreglen i udvidet omfang, dvs. i alle de (teknisk) tilgængelige systemer. Øvrige sundhedspersoner kan foretage opslag efter værdispringsreglen efter deres autorisation, dog er adgangen ikke begrænset til oplysninger om aktuel behandling.

Det er således et lovkrav, at EPJ-systemerne er indrettet til at kunne håndtere, at sundhedspersoner kan få adgang til EPJ, i de situationer, hvor værdispringsreglen finder anvendelse. Den enkelte sundhedspersons opslag (behandling af data) skal markeres i loggen, så den let kan gøres til genstand for nærmere analyse og evt. rapportering som beskrevet i sikkerhedsorganisationens procedurer.

En særlig situation, som der via adgangsstyringen skal tages højde for, er lægens eller den sygehusansatte tandlæges mulighed for med patientens samtykke ved opslag i EPJ at indhente oplysninger i forbindelse med behandling af patienter, men hvor opslaget ikke er nødvendigt – eller ikke relevant - i forbindelse med den igangværende behandling.

Ønsker en patient fx at få at vide, hvilke undersøgelser patienten fik foretaget for år tilbage relateret til et afsluttet behandlingsforløb, kan lægen undersøge dette ved opslag i EPJ med patientens samtykke. Adgangen til at indhente er bred, dvs., det

er en adgang til både aktuelle og historiske data og efter omstændighederne adgang til at søge på tværs af organisatoriske grænser og sektorer i den udstrækning, systemerne teknisk giver mulighed herfor. Sundhedsloven stiller således krav om, at EPJ-systemerne skal kunne administrere og ajourføre patientens samtykke.

Udover omfanget af autoriseringen er typen af autorisation også central i forbindelse med tildeling af autorisation. Overordnet set findes der følgende kategorier af autorisering:

Typer af autorisering

Der skal benyttes følgende typer af autorisering:

Almindelig autorisering omfatter adgang til data om patienter og til funktionaliteter, der behandler data for flere patienter af gangen tilknyttet egen behandlingsenhed. Det drejer sig fx om søgninger, sammenstilling af lister og generering af rapporter. Vikarer, der ansættes for en måned eller længere, gives 'almindelig autorisering'. Autoriseringen til en eller flere patienters data skal kunne begrænses i overensstemmelse med patienters evt. tilkendegivelse om, at nærmere angivne sundhedspersoner nægtes adgang til deres helbredsoplysninger, jf. nedenfor om patienters mulighed for at frabede sig indhentning af oplysninger. Systemmæssigt kan adgangsbegrænsningen knyttes til de pågældende patientdata, så den kan gøres gældende for dele af en patients helbredsoplysninger, og så dens iværksættelse ikke kræver ændring i autoriseringsoplysningerne om hver enkelt sundhedsperson.

Midlertidig autorisering (fx tilsyn og anden specialebistand) Autoriseringstypen bør normalt kun udstedes af det sundhedsfaglige personale på den organisatoriske enhed, hvortil patienten er knyttet, og tænkes benyttet, når der rekvireres sundhedsfaglig assistance fra en anden enhed. Denne autorisering har samme omfang med hensyn til data og funktionaliteter som 'almindelig autorisering', men den er begrænset til et tidsrum, der er relevant for udførelsen af den tilsigtede assistance, fx et døgn eller en uge. Midlertidig autorisering kan gives døgnet rundt, og kan anvendes til korttidsvikarer.

Autorisering til udvidet tværgående databehandling Denne autorisering har normalt samme omfang med hensyn til typer af information som 'almindelig autorisering', men den omfatter tillige ret til at anvende funktionaliteter, der kan behandle data om flere patienter på én gang ud over grænserne for medarbejderens egen behandlingsenhed. Autoriseringstypen skal kun anvendes til personer, der har vedvarende arbejdsopgaver, der kræver en sådan tværgående tilgang til patientdata, fx i forbindelse med ledelse og planlægning. En tilsvarende, men tidsbegrænset autorisering kan gives af den organisatoriske enheds ledelse til personer med opgaver inden for fx kvalitetsudvikling og forskning. Autoriseringen gives i overensstemmelse med en godkendt protokol for aktiviteten. Behandling af data iht. denne autoriseringstype skal markeres særligt i loggen.

Autorisering til data i forbindelse med øjeblikkeligt patientbehandlingsbehov
I meget hastende tilfælde, fx ved behandling af en patient med hjertestop, skal det være muligt for enhver sundhedsperson efter værdispringsreglen at indhente oplysninger om patienten. Denne type behandling af data, som sundhedspersonen ikke har normal adgangstilladelse til, skal markeres i loggen, så den let kan gøres til genstand for nærmere analyse og rapportering som beskrevet i sikkerhedsorganisationens procedurer. Det kan i praksis foregå ved brug af en særlig 'knap' i bruger-

fladen, der giver adgang til at finde evt. oplysninger, en bruger ikke normalt er autoriseret til.

Selve tildelingen af adgangskoder skal styres ved en formaliseret proces og brugernes adgangsrettigheder skal gennemgås regelmæssigt efter en formaliseret fremgangsmåde.

Patientens mulighed for at frabede sig indhentning af helbredsoplysninger m.v. efter sundhedsloven

Efter sundhedsloven har patienter ret til at frabede sig, at en sundhedsperson indhenter oplysninger i forbindelse med aktuel behandling. Patientens ret til at sige fra over for indhentning af oplysninger fra EPJ-systemer gør, at EPJ-systemerne skal kunne håndtere, at der teknisk blokeres for opslag i overensstemmelse med patientens ønsker. Sundhedsloven indeholder således et krav om blokering af adgang til opslag i EPJ-systemer i de tilfælde, hvor patienter har tilkendegivet, at de ikke ønsker, at der indhentes helbredsoplysninger til brug for en aktuel behandling.

Eksempelvis kan en patient frabede sig, at læge X indhenter oplysninger om patienten.

Den tekniske udvikling vil kunne medføre, at patienten får mulighed for at frabede sig indhentning af bestemte oplysninger eller bestemte kategorier af oplysninger, fx alle psykiatriske oplysninger. Dette vil medføre et krav om, at systemerne skal kunne administrere patientens ønsker om, at der ikke indhentes bestemte - kategorier af - oplysninger.

Det vil sige, at sundhedsloven stiller krav om, at i det omfang systemerne kan håndtere selektiv frasigelse, skal systemerne kunne håndtere det.

3.8.3 Brugernes ansvar

Brugerne skal gøres opmærksomme på deres ansvar, specielt vedrørende personlige adgangskoder og informationsbehandlingsudstyr. Det skal herudover indskærpes, at fortrolige og følsomme oplysninger på papir eller andre medier ikke må kunne misbruges.

De ansatte i sundhedsvæsenet og særligt sundhedspersoner skal have kendskab til og viden om de nye regler om sundhedspersoners juridiske og tekniske adgang til EPJ-systemer. Det anbefales, at ledelsen på sygehusene, klinikkerne m.v. udarbejder instrukser til medarbejderne om betydningen af de nye regler. Ledelsen bør informere om den nye, skærpede straffebestemmelse i sundhedslovens § 271, der hjemler bødestraf eller fængsel indtil 4 måneder.

3.8.4 Styring af netværksadgang

Formålet er at beskytte både interne og eksterne netværkstjenester mod uautoriseret adgang.

3.8.5 Styring af systemadgang

Formålet med styring af systemadgang er at forhindre uautoriseret adgang til informationsbehandlingssystemer. Systemadgang skal beskyttes af en sikker log-on-procedure. I den forbindelse er det vigtigt at tage hensyn til, at sundhedsfagligt personale typisk har brug for at logge sig på et meget stort antal gange i løbet af en arbejdsdag - log-on eller log-off bør ikke tage mere end få sekunder.

Kombinationen af brugernavn og passwords kan give tilstrækkelig sikker person-identifikation til brugere i forbindelse med sundhedsvæsenets it-systemer. Der skal ikke benyttes gruppe-identifikation og fælles password for flere brugere, da den enkelte brugers adgang til patientdata skal kunne spores.

3.8.6 Mobilt udstyr og fjernarbejdspladser

Formålet er at beskytte organisationens informationer ved brugen af mobilt udstyr og fjernarbejdspladser. Mobilt udstyr og fjernarbejdspladser skaber behov for yderligere sikringsforanstaltninger, da anvendelsen finder sted uden for organisationens kontrollerede område.

Mobilt udstyr

Der skal være retningslinjer for anvendelsen af mobilt udstyr (fx PDA'er (Personal Digital Assistent), bærbare Pc'er og mobiltelefoner) uden for organisationens kontrollerede område, og de nødvendige beskyttelsesforanstaltninger – herunder kryptering – skal være etableret. Mobilt udstyr med netværksforbindelse via et trådløst netværk er udsat for en særlig risiko, som skal indgå i valget af beskyttelsesforanstaltninger.

Mobilt udstyr, der anvendes udenfor organisationens rammer, er særligt udsat for ødelæggelse, tab og tyveri. Derfor skal særlige sikringsforanstaltninger overvejes i denne forbindelse. Som eksempler på sådanne sikringsforanstaltninger kan nævnes:

- Passwords, der låser for brug til apparaturet både på hardware-, applikations- og operativsystemniveau
- Regelmæssig synkronisering med centrale systemer
- Regelmæssig (automatisk) sletning af følsomme data
- Begrænsning af datalagring på mobile enheder

Persondata, der opbevares på flytbare datamedier (fx bærbare computere, lommecomputere (PDA'er), Cd-rom, disketter), skal krypteres[10]. For følsomme personoplysninger skal anvendes stærk kryptering med en anerkendt algoritme.

Ved stærk kryptering forstår Datatilsynet en kryptering, der på det givne tidspunkt i it-sikkerhedsbranchen i almindelighed anerkendes som værende stærk.

Fjernarbejdsplader

Fjernarbejdspladser skal kun tillades, hvis der kan etableres tilfredsstillende beskyttelse af organisationens informationer. Fjernarbejdspladser skal autoriseres og sty-

res af ledelsen, som skal sikre sig, at det fastlagte sikkerhedsniveau kan fastholdes. Fjernarbejde med helbredsoplysninger kan bl.a. forekomme i forbindelse med telemedicin, vagttjeneste (røntgen- og andre billedundersøgelser, blodprøvesvar, EKG m.v.) og ved planlægnings-, forsknings- og kvalitetsudviklingsopgaver.

Af Datatilsynets sikkerhedsbekendtgørelse, jf. § 7, stk. 2, følger det, at hvis behandling af personoplysninger finder sted på en pc-arbejdsplads uden for den dataansvarlige myndigheds lokaliteter, skal myndigheden fastsætte særlige retningslinier herfor, således at det sikres, at bestemmelserne om sikkerhedsforanstaltninger iagttages. Nogle af de sikkerhedsmæssige områder, der skal tages stilling til, er lokal lagring af oplysninger, lokal udskrivning af oplysninger og fysisk sikkerhed.

For så vidt angår definitionen af ´fjernarbejdspladser` er det i Datatilsynets sikkerhedsvejledning anført, at der ved pc-arbejdspladser uden for den dataansvarliges lokaliteter først og fremmest tænkes på hjemmearbejdspladser (arbejdsplads som etableres ved opstilling i en medarbejders hjem af en pc med forbindelse til arbejdsgiverens it-system, således at medarbejderen kan udføre visse arbejdsopgaver hjemmefra). Det fremgår endvidere, at bestemmelsen også vil gælde i en række andre tilfælde, hvor behandling foretages andre steder end ved de sædvanlige arbejdspladser på arbejdsgiverens lokaliteter (brug af bærbare pc'er under rejse, hos kunder eller klienter etc., anvendelse af en pc i en anden organisation eller myndighed, anvendelse af privat pc i hjemmet). Dette gælder ikke alene for pc'er, men også for andet elektronisk udstyr, fx PDA'er og lignende.

Det skal anføres, at dersom forbindelse af fjernarbejdspladsen og det centrale system sker ved brug af en åben (fx internet-) forbindelse, skal persondata transmitteres i stærkt krypteret tilstand.

3.9 Anskaffelse, udvikling og vedligehold af informationssystemer

3.9.1 Sikkerhedskrav til informationssystemer

Informationsbehandlingssystemer omfatter styresystemer, infrastruktur, driftssystemer (både egenudviklede systemer og hyldevare-systemer), brugerudviklede systemer og tjenesteydelser. I sundhedsvæsenet er PAS (Patientadministrative systemer)-systemer, medicinmoduler, praksissystemer, laboratoriesystemer og medikotekniske systemer eksempler på informationssystemer.

Kravene til sikkerhed skal være identificeret og aftalt før udvikling og implementering af informationsbehandlingssystemer. Alle krav til sikkerhed, inklusiv behovet for at gå tilbage til tidligere versioner, skal være identificeret i forbindelse med kravspecifikationen i et projekt. Sikkerhedskravene skal være begrundede, aftalte og dokumenterede, som en naturlig del af den driftsmæssige begrundelse for systemet.

Krav til sikkerhed samt forretningsgange for implementering af sikkerhed skal integreres i de tidlige faser af informationsbehandlingsprojekter. Sikringsforanstaltninger, der implementeres i starten, er betydeligt billigere at implementere og vedligeholde end foranstaltninger, der implementeres efterfølgende.

3.9.2 Korrekt informationsbehandling

Formålet med korrekt informationsbehandling er at forhindre fejl, tab, uautoriserede ændringer eller misbrug af informationer i systemerne. Sikringsforanstaltningerne indenfor dette område omfatter valideringen af data, der sendes ind i systemet, intern databehandling samt de data, der efterfølgende leveres af systemet.

Yderligere sikringsforanstaltninger skal implementeres, hvor databehandlingen kan have indflydelse på følsomme, værdifulde eller kritiske informationsaktiver. Sådanne sikringsforanstaltninger skal implementeres på baggrund af kravene til systemets sikkerhed samt risikovurderinger for systemet.

Data, der sendes ind i systemerne, skal valideres for korrekthed. Der skal være inddatakontroller for fx stamdata (navne, adresser, m.m.), og det skal vurderes, hvilke af følgende kontroller der er nødvendige. Det kan fx dreje sig om indtastningskontroller såsom grænsekontroller eller begrænsning af felter til specificerede grænseværdier med det formål at undgå data uden for tilladte værdier eller formater, fx at der kun kan indtastes tal i numeriske felter, og at der ikke kan registreres umulige biologiske værdier, fx blodtryk: -22/10000.

Kontrol af datas korrekthed skal indarbejdes i organisationens systemer med det formål at afsløre, om data er blevet modificeret, enten på grund af systemfejl eller bevidste handlinger. Specielt følgende områder skal vurderes i forbindelse med udvikling og implementering af informationsbehandlingssystemer: Brugen af funktionerne tilføj, rediger og slet data. Der skal sikres mod fejl gennem kontrol af integriteten, autenticiteten eller andre sikkerhedskontroller af data, der er hentet via netværksforbindelser.

Der skal stilles krav til sikring af datas autenticitet og integritet i elektroniske meddelelser. Kryptografi og lukkede netværk kan anvendes som et hensigtsmæssigt værktøj til at sikre meddelelsers integritet.

Uddata fra systemer skal valideres med det formål at sikre, at de, under de givne omstændigheder, er korrekte. Valideringen kan omfatte sandsynlighedskontrol for at kontrollere, om data er fornuftige, fx om data giver klinisk mening.

3.9.3 Kryptografi

Formålet med kryptografi er at sikre fortrolighed, autenticitet og integritet af informationer ved hjælp af kryptografiske metoder. Ved kryptering skaber man en kodet tekst, der kun kan afkodes af den, som er i besiddelse af den rigtige nøgle.

Kryptografi kan anvendes til at opnå flere forskellige formål:

- Fortrolighed: Til sikring af følsomme og kritiske informationer, både lagrede og transmitterede informationer.
- Integritet og autenticitet: Ved anvendelse af digital signatur (OCES) kan både autenticiteten og integriteten sikres.
- Uafviselighed: Ved anvendelse af krypteringsteknikker kan der opnås vished for, om en hændelse eller en handling har eller ikke har fundet sted.

Der skal være etableret et nøglehåndteringssystem til støtte for anvendelsen af kryptografi. I dokumentationer til OCES ligger retningslinier for håndtering af digitale certifikater og de dertil knyttede krypteringsnøgler.

3.9.4 Styring af driftsmiljøet

Formålet med styring af driftsmiljøet er at sikre de systemtekniske filer i driftsmiljøet. Dette kan bl.a. opnås gennem, at styresystemer og brugersystemer kun må implementeres efter tilstrækkelige og tilfredsstillende test. Testen skal indeholde test af brugbarhed, sikkerhed, indvirkning på andre systemer og brugervenlighed og skal udføres i et separat miljø – et testmiljø. Der skal være en plan for tilbagerulning, før ændringer implementeres.

Leverandører må kun få fysisk eller netværksbaseret adgang, når det er nødvendigt, og det må kun finde sted med ledelsens accept. Leverandørers aktiviteter skal overvåges, ligesom eksternt leverede systemer skal overvåges og kontrolleres.

Data, der anvendes til test, skal udvælges omhyggeligt, kontrolleres nøje og beskyttes i henhold til dets klassifikation. System- og driftoverdragelsestest stiller ofte krav til store mængder testdata, der ligner ægte data fra driftsmiljøet. Driftsdatabaser med personfølsomme eller andre kritiske informationer, dvs. patienters helbredsoplysninger, må ikke anvendes til test. Hvis der er behov for at anvende personfølsomme informationer, skal disse informationer ændres i en sådan grad, at de ikke længere kan genkendes og henføres til personer, før de anvendes til test.

Kildekode er den kode, systemudviklerne bruger til detailspecifikation af en løsning. Koden oversættes og bindes sammen således, at der skabes eksekverbare filer.

Adgang til kildekode og den tilhørende dokumentation, fx designspecifikationer, diagrammer og testplaner, skal kontrolleres strengt for at forhindre uautoriseret funktionalitet og utilsigtede ændringer. For kildekode til programmer kan dette opnås ved at lagre kildekoden under streng kontrol, helst i særlige kildebiblioteker.

3.9.5 Sikkerhed i udviklings- og hjælpeprocesser

Formålet er at opretholde sikkerheden i virksomhedens brugersystemer gennem at holde udviklings- og hjælpemiljøer under streng kontrol. Ejerne af brugersystemer, er også ansvarlige for de hertil knyttede udviklings- og hjælpemiljøer.

Der skal være udarbejdet formelle forretningsgange for ændringsstyring. Disse skal være implementeret således, at risikoen for kompromittering af virksomhedens informationer minimeres. Introduktion af nye systemer og større ændringer til de eksisterende systemer skal følge en formel forretningsgang med dokumentation, specifikationer, test, kvalitetskontrol og styret implementering.

Der skal implementeres beskyttelsesforanstaltninger, der begrænser risikoen for lækage af informationer gennem fx skjulte kanaler, herunder jævnlig overvågning af medarbejdere og systemer, hvor lovgivningen tillader det.

3.9.6 Sårbarhedsstyring

En opdateret og fuldstændig liste over virksomhedens informationsaktiver er en forudsætning for en effektiv sikring mod sårbarheder. Specifikke informationer om mulige sårbarheder inkluderer producenten, versionsnummeret, en liste over, hvilke systemkomponenter der er installeret på hvilke systemer, samt en liste over de medarbejdere, der er ansvarlige for systemkomponenterne.

3.10 Styring af sikkerhedshændelser

Formålet er at opnå, at sikkerhedshændelser og svagheder i virksomhedens informationsbehandlingssystemer rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Forretningsgange for rapportering og eskalering skal være på plads. Alle medarbejdere, samarbejdspartnere og øvrige brugere skal være bekendt med forretningsgangene for rapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden for virksomhedens aktiver. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til et enkelt udpeget kontaktpunkt.

Alle medarbejdere, samarbejdspartnere og andre brugere skal rapportere disse ting enten til ledelsen eller direkte til deres eksterne leverandør hurtigst muligt med det formål at forhindre sikkerhedsbrud. Rapporteringsproceduren skal være så let og tilgængelig som muligt. De skal informeres om, at de ikke under nogen omstændigheder selv skal forsøge at bevise en mistænkt svaghed.

3.10.1 Håndtering af sikkerhedsbrud og forbedringer

Formålet er at sikre en ensartet og effektiv håndtering af sikkerhedsbrud. Ansvar og procedurer for håndteringen af sikkerhedsbrud og svagheder skal være på plads, således at disse kan håndteres effektivt, når de opstår. Der skal være etableret en proces til løbende forbedringer af reaktioner på, overvågning af og vurdering af sikkerhedsbrud.

3.11 Beredskabsstyring

Formålet er at beredskabsstyring skal:

- modvirke afbrydelser i virksomhedens forretningsaktiviteter
- beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe og
- sikrer en hurtig retablering

Organisationen skal implementere beredskabsstyring som en løbende opgave med det formål at begrænse konsekvenserne af tab af informationsaktiver forårsaget af katastrofer og sikkerhedsbrister til et acceptabelt niveau samt at genoprette situationen gennem en kombination af forebyggende og udbedrende foranstaltninger. I forbindelse med beredskabsstyringen skal organisationens kritiske driftssaktiviteter identificeres, og beredskabskravene vedrørende informationssikkerhed skal inte-

greres med andre beredskabskrav vedrørende drift, personale, materiel, transport og øvrige faciliteter.

3.12 Overensstemmelse med lovbestemte og kontraktlige krav

Formålet med denne gruppe af sikringsforanstaltninger er at forhindre brud på relevante sikkerhedskrav i lovgivningen og administrative forskrifter samt i indgåede kontraktlige forpligtelser.

3.12.1 Overensstemmelse med lovbestemte krav

Af bestemmelserne i sikkerhedsbekendtgørelsen fremgår det, at den dataansvarlige myndighed skal fastsætte nærmere interne bestemmelser om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, der fremgår af bekendtgørelsen. Bestemmelserne skal navnlig omfatte organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer. Der skal endvidere fastsættes instrukser, som fastlægger ansvaret for og beskriver behandling og destruktion af ind- og uddatamateriale samt anvendelse af edb-udstyr. Desuden skal der fastsættes retningslinier for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat for myndigheden.

Sikkerhedsbekendtgørelsen retter sig imod behandling af oplysninger, der føres for den offentlige forvaltning, men det er som tidligere nævnt Datatilsynets anbefaling, at der i videst muligt omfang tilrettelægges sikkerhedsforanstaltninger i overensstemmelse med bekendtgørelsen i forbindelse med private dataansvarliges behandling af personoplysninger.

Da bestemmelserne i sikkerhedsbekendtgørelsen er af mere generel og overordnet karakter, vil der være behov for, at den enkelte dataansvarlige myndighed nærmere fastlægger og beskriver, hvorledes bekendtgørelsens bestemmelser er tænkt opfyldt, og i det hele taget, hvorledes sikkerhedsarbejdet i forbindelse med behandling af personoplysninger tilrettelægges.

Udover at tjene som dokumentation vil de bestemmelser m.v., som den dataansvarlige myndighed udarbejder, også kunne tjene som arbejdsgangsbeskrivelser, funktionsbeskrivelser for forskellige funktioner i sikkerhedsarbejdet, ansvarsbeskrivelse og -afgrænsning m.m.

Visse af de nævnte beskrivelser kan være af en sådan karakter, at sikkerhedsmæssige hensyn taler for at klassificere dem som ikke offentligt tilgængelige. Dette kan være aktuelt for fx beskrivelse af tekniske indretninger såsom alarmsystemer.

Da dokumentation er uden værdi, hvis den ikke er aktuel, bør de interne bestemmelser løbende ajourføres, således at de til enhver tid afspejler de faktiske forhold på stedet.

Det påhviler den dataansvarlige at kontrollere mindst en gang årligt, at den nævnte ajourføring af de interne bestemmelser er foretaget.

3.12.1.1 Beskyttelse af personoplysninger

Langt de fleste af de informationer, der benyttes i sundhedsvæsenet, er følsomme personoplysninger. Ud over persondatalovens bestemmelser findes for sundhedsvæsenet en række bestemmelser i sundhedsloven, der regulerer behandlingen af patientdata. Disse regler er beskrevet under pkt. 2.3 samt under pkt. 3.8.

Journalføring

Reglerne om journalføring findes i autorisationsloven og de administrative forskrifter, der er fastsat for forskellige sundhedsfaglige personalegrupper.

Reglerne regulerer bl.a., i hvilket omfang sundhedspersoner skal journalføre i patientjournaler, hvor lang tid patientjournaler skal opbevares, og hvordan rettelser skal foretages i patientjournaler. Der er pligt til at journalføre bestemte oplysninger og specifikke patientrettigheder.

Patientjournaler skal som udgangspunkt opbevares i mindst 10 år (opbevaringsperioden) fra den seneste optegnelse i patientjournalen. For visse personalegruppers patientjournaler er der fastsat en kortere opbevaringsperiode.

Journalføringsreglerne stiller krav om, at det ikke må være muligt at slette i patientjournalerne. I en elektronisk patientjournal skal den oprindelige version af de oplysninger, der er ændret ved at rette eller tilføje, fortsat være tilgængelig[p]. Er det nødvendigt at rette eller tilføje i patientjournalen, skal det derfor ske på en sådan måde, at den oprindelige tekst bevares.

Der findes særlige regler om bevaring og kassation i arkivloven og de i medfør af denne fastsatte administrative forskrifter.

[p] Jf. autorisationslovens § 24

4 Bilag

4.1 Bilag 1: Ord- og begrebsforklaring

Adgangsbegrænsning	En funktionalitet, der teknisk sætter grænserne for, hvilke data i et IT-system en given bruger kan få adgang til at behandle, samt hvilken form for behandling vedkommende kan udføre på disse data.
Anonymisering	Anonymisering foreligger, når det ikke på nogen måde for nogen som helst er muligt at henføre data til en bestemt person. Bemærk, at dette i nogle tilfælde er et mere vidtgående krav end fjernelse af navn og CPR-nummer. Ved afgørelsen af, om en person er identificerbar, skal alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den dataansvarlige eller af enhver anden person, tages i betragtning.
Autenticitet	Garanti for identitet i forholdet til et IT-system.
Autentificering	En vigtig egenskab ved adgangskontrol er, at den omfatter en autentificering af de personer, som gives adgang til data. Autentificering fastslår, at en bruger er identisk med den person, vedkommende oplyser at være.
Autorisation	Den sundhedsfaglige autorisation, som af Sundhedsstyrelsen tildeles visse sundhedspersoner, fx læger og sygeplejersker. Må i denne vejledning ikke forveksles med autorisering.
Autorisering	I denne vejledning benyttet om et grundlæggende begreb for opretholdelse af it-sikkerhed omkring patientoplysninger. Autorisering indebærer ret til at udføre en nærmere angivet form for behandling af nærmere angivne data vedr. nærmere angivne personer i et nærmere angivet tidsrum og til et formål, der sædvanligvis bestemmes af den autoriseredes professionelle rolle. Må i denne vejledning ikke forveksles med autorisation. Se også autenticitet.
Behandlingsenhed	Ved udtrykket behandlingsenhed forstås sygehus, sygehusafdeling, afsnit, klinik el. lign. Kravet om tilknytning til samme behandlingsenhed efter sundhedslovens § 42 a, stk. 2, indebærer et krav om, at sundhedspersonen og patienten er tilknyttet samme organisatoriske enhed, hvor der udføres sundhedsfaglig virksomhed (fx afdeling, klinik, skadestue).
Data	Udtrykket 'data' angiver et lavt abstraktionsniveau, typisk 'selve indholdet i et databasefelt'. Vha. data kan der dannes information, som er 'noget, man forstår', fx indholdet i et databasefelt kombineret med viden om, hvad feltet skal beskrive. Se også 'information'.
Dataansvarlig	Ved begrebet dataansvarlig forstås den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger (persondatalovens § 3, nr. 4).

Databehandler	Ved begrebet databehandler forstås den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne (persondatalovens § 3, nr. 5).
Databehandling	I sammenhæng med informationssikkerhed anvendes betegnelsen behandling (af data eller information) i den videst tænkelige betydning - ligesom i persondataloven. Udtrykket 'behandling' dækker over enhver form for måde at håndtere oplysninger om personer på, fx indsamling, registrering, systematisering, opbevaring, ændring, søgning, transmission, overladelse, videregivelse, sammenstilling, samkøring, blokering, sletning eller tilintetgørelse. Har man indhentet data, har man altså 'behandlet' dem.
Elektroniske systemer	Digitale systemer til behandling af data. Anvendelsesområdet for §§ 42 a og 42 b i sundhedsloven er indhentning af oplysninger ved opslag i elektroniske systemer i det danske sundhedsvæsen, der indeholder helbredsoplysninger m.v., der er indsamlet til det formål at understøtte den sundhedsfaglige behandling af de registrerede patienter eller til formål, der ikke er uforenelige hermed, fx Landspatientregisteret. Papirjournaler (manuelle patientjournaler) er ikke omfattet af reglerne. De nye regler regulerer opslag i elektroniske systemer, (sygehusenes og hjemmesygeplejens elektroniske systemer etc.), medmindre der findes særlige regler om adgang til bestemte systemer, som fx den Personlige Elektroniske Medicinprofil, som reguleres af sundhedslovens § 157. Se også 'EPJ-system'
EPJ (Elektronisk Patientjournal)	En EPJ er den logiske afgrænsede mængde helbredsinformationer og andre klinisk relevante oplysninger om en person, som et EPJ-system kan behandle, dvs. registrere, lagre, bearbejde, præsentere m.v.
EPJ-system	Et EPJ-system er et elektronisk informationssystem, som til støtte for undersøgelse, behandling, pleje og rehabilitering kan behandle data dvs. registrere, lagre, bearbejde, præsentere m.v., der ligger til grund for enkeltpersoners helbredsinformationer og andre klinisk relevante oplysninger.
Fortrolighed	Sikkerhed for, at ingen uvedkommende får kendskab til den pågældende information.
Følsomme oplysninger	Oplysninger af følsom karakter (persondataloven § 7, stk. 1: oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold) og § 8, stk. 1: oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte.
Identificerbar person	Se bemærkning under "Personoplysninger"

Helbredsoplysninger m.v.	Efter sundhedslovens § 41, stk. 1, defineres begrebet *helbredsoplysninger m.v.* som oplysninger om patientens helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger. Også oplysninger om, hvor der er registreret oplysninger om en persons helbredsforhold er omfattet. Helbredsforhold er sygdomsoplysninger eller oplysninger om en persons helbredstilstand. Omfattet er oplysninger om en persons tidligere, nuværende og fremtidige fysiske og psykiske helbredstilstand.
Indhentning (af helbredsoplysninger)	Indhentningsreglerne gælder ved ethvert opslag, en sundhedsperson foretager i et elektronisk system, hvori der er lagret helbredsoplysninger m.v. Eksempelvis vil indhentningsreglerne gælde, når en læge via brugerstyring foretager et opslag i et EPJ-system. Der vil ligeledes være tale om en indhentning, der reguleres af § 42 a, når en ansat sundhedsperson i den kommunale hjemmesygepleje foretager et opslag i et elektronisk patientjournalsystem, fx via en håndholdt PDA. Indhentningsreglerne[q] giver kun adgang til selve opslaget og ikke den efterfølgende evt. anvendelse af oplysningerne, der involverer andre sundhedspersoner. En indhentning ved opslag er kendetegnet ved at være en selvstændig handling fra sundhedspersonen, hvor oplysningen kun bliver tilgængelig for den indhentende sundhedsperson. Videreformidler sundhedspersonen de indhentede oplysninger til andre sundhedspersoner, vil der derfor være tale om en videregivelse, som er omfattet af videregivelsesreglerne.
Information	Ved udtrykket 'information' forstås data i en sammenhæng, så det giver mening. Information og oplysning er synonymer. Se også 'data'.
Informationsbehandlingssystem	Synonymt med 'informationssystem'. Ethvert system, der i persondatalovens forstand kan behandle informationer. Se også 'Databehandling' og 'Information'.
Integritet	Det forhold, at information ikke er illegitimt ændret, bevidst eller ubevidst.
Kryptering af data	Kodning af data, så de bliver uforståelige. Kun ved brug af en nærmere bestemt nøgle kan afkodning finde sted, så data bliver forståelige.
Logning	En forud fastlagt og automatisk registrering af oplysninger om datas behandling.
Log-on / Log-off	Procedurer, der indleder og afsluttet en brugers aktivitet i relation til et eller flere IT-systemer med adgangsbegrænsning og/eller logning af brugeraktivitet. Synonyme med 'login / logout'
Lukkede systemer	Herved forstås behandlingssteders elektroniske systemer, der kun indeholder oplysninger til brug for behandling, som gives på det pågældende behandlingssted.

[q] Sundhedslovens §§ 42 a og 42 b

Oplysning	Ved udtrykket 'oplysning' forstås data i en sammenhæng, så det giver mening. Information og oplysning er synonymer. Se også 'data'.
Organisatorisk enhed	I denne vejledning benyttet i betydningen afdeling, klinik, skadestue, ambulatorium eller lignende.
Password (kodeord)	Streng af tegn (bogstaver, tal eller symboler), der kan bidrage til sikring af brugerens autenticitet (se dette). Bruges typisk ved, at brugeren sammen med sit navn (evt. brugernavn eller –ID) oplyser et password (kodeord), som kun er kendt af brugeren selv og af IT-systemet. Evt. kan i stedet anvendes en genstand ('token'), som kun denne bruger har, fx en nøgle, et magnetkort eller et såkaldt 'smart card', der benyttes som en slags elektronisk nøgle over for systemet.
Patientbehandling	Henviser til behandling i sundhedslovens forstand, hvor behandling omfatter undersøgelse, diagnosticering, sygdomsbehandling, fødselshjælp, genoptræning, sundhedsfaglig pleje samt forebyggelse og sundhedsfremme i forhold til den enkelte patient (sundhedslovens § 5).
Patientdata	Data, der kan henføres til en patient.
Patientforløb	En del af et sygdomsforløb, hvor en patient er i kontakt med sundhedsvæsenet for samme helbredsproblem.
PDA	Personal digital assistant. Et (almindeligvis håndholdt) elektronisk hjælpemiddel, der indeholder funktioner fra en computer, mobiltelefon, musikafspiller, kamera m.m.
Personoplysninger	'Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).' Persondatalovens § 3, nr. 1 Omfattet af begrebet personoplysninger er således oplysninger, som kan henføres til en fysisk person, selv om dette forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer som fx løbenummer. Omfattet vil ligeledes bl.a. være oplysninger, som foreligger i form af billede, personens stemme, fingeraftryk eller genetiske kendetegn, hvis det i praksis er muligt at henføre oplysningerne til en bestemt fysisk person.
Register	Register med personoplysninger (register): Enhver struktureret samling af personoplysninger, der er tilgængelige efter bestemte kriterier, hvad enten denne samling er placeret centralt, decentralt eller er fordelt på et funktionsbestemt eller geografisk grundlag. Persondataloven § 3, nr. 3.
Sikkerhedsforanstaltning	Synonymt med 'sikringsforanstaltning', som er udtrykket, der benyttes i den danske standard for informationssikkerhed DS 484 og nævnes på http://begrebsbasen.sst.dk som den 'foretrukne term'.
Sikkerhedshændelse	Hændelse af betydning for sikkerheden.

Sikringsforanstaltning	Det Nationale Begrebsråd for Sundhedsvæsenet definerer begrebet således: 'foranstaltning der har til formål at øge informationssikkerhed'
Sporbarhed	Mulighed for konstatering af, hvilken behandling data er blevet underkastet og af hvem.
Sundhedsperson	Ved en *sundhedsperson* forstås personer, der er autoriserede i henhold til særlig lovgivning til at varetage sundhedsfaglige opgaver, og personer, der handler på disses ansvar, jf. sundhedslovens § 6. Det er en betingelse, at den ansatte aktivt udfører eller medvirker ved patientbehandlingen for at kunne defineres som en sundhedsperson. Det afhænger af en konkret vurdering, om en ansat i sundhedsvæsenet udfører opgaver, der gør, at vedkommende kan defineres som sundhedsperson. Elever og studerende vil også kunne være sundhedspersoner, hvis ovennævnte betingelser er opfyldt.
Sygdomsforløb	En periode i hvilken en person har en sygdom eller et andet helbredsproblem.
Tilgængelighed	Et begreb, der udtrykker, hvor let og hyppigt man kan få adgang til data i situationer, hvor man har brug for det.
Videregivelse (af helbredsoplysninger)	Videregivelsesreglerne[r] gælder for enhver videregivelse af oplysninger i forbindelse med behandling af patienter, dvs. for enhver anden form for udveksling af oplysninger, end den, indhentningsreglerne giver adgang til. Dette gælder, uanset hvilket medie oplysningerne stammer fra eller udveksles ved hjælp af. Mundtlig videreformidling af oplysninger, der hidrører fra opslag i det elektroniske system, er derfor omfattet af videregivelsesreglerne. Videregivelse af et print af oplysningerne fra opslaget i det elektroniske system er også reguleret af videregivelsesreglerne, uanset om videregivelsen af printet sker elektronisk (scannes) eller manuelt (fysisk). Videregivelsesreglerne finder endvidere anvendelse på enhver form for videregivelse af papirjournaler eller af skriftligt print fra papirjournaler eller mundtlig videreformidling af oplysninger fra papirjournal.
Uafviselighed	Det forhold, at der ikke efterfølgende kan rejses tvivl om, hvem der har foretaget en nærmere bestemt behandling af data, eller om den overhovedet har fundet sted. Hvis logning kombineres med en forudgående sikring af brugerens autenticitet, vil logningen samtidig sikre de registrerede behandlingers uafviselighed. At man således er i stand til at fastslå, om en behandling af data er foretaget af en person, som er autoriseret dertil, er et væsentligt element i sikringen af datas integritet (se dette).

[r] Sundhedslovens §§ 41 og 42

4.2 Bilag 2: Referenceliste

For så vidt angår referencer til love bemærkes det, at lovene og samtlige vedtagne lovændringer er tilgængelige på www.retsinformation.dk. Lovene findes ved at taste lovens nr. og året for vedtagelsen i feltet øverst til venstre.

---

[1] EPJ-Observatoriets Statusrapport 2002, EPJ-Observatoriet, oktober 2002 og EPJ-Observatoriets statusbeskrivelser i amterne 2006, EPJ-Observatoriet, oktober 2006

[2] MedCom status på www.medcom.dk (3.9.2007)

[3] Lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed, Lov nr. 451 af 22. maj 2006

[4] Sundhedsloven, Lov nr. 546 af 24. juni 2005, med senere ændringer

[5] Lov nr. 431 af 8. maj 2007 om ændring af sundhedsloven

[6] Strategi for digitalisering af den offentlige sektor 2007-2010 – Mod bedre digital service, øget effektivisering og stærkere samarbejde, Regeringen, KL og Danske Regioner, juni 2007

[7] Standard for informationssikkerhed, DS 484 1. udgave, Dansk Standard, 20. september 2005

[8] Lov om behandling af personoplysninger (persondataloven), Lov nr. 429 af 31. maj 2000 med senere ændringer

[9] Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen), Bekendtgørelse nr. 528 af 15. juni 2000

[10] Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsvejledningen), Vejledning nr. 37 af 2. april 2001

[11] Notat om Sikkerhed ved transmission af personoplysninger via internettet i den private sektor, Datatilsynet, 1. juni 2007

[12] Bekendtgørelse om lægers, tandlægers, kiropraktorers, jordemødres, kliniske diætisters, kliniske tandteknikeres, tandplejeres, optikeres og kontaktlinseoptikeres patientjournaler (journalføring, opbevaring, videregivelse og overdragelse m.v.), Bekendtgørelse nr. 1373 af 12. december 2006

[13] Lov om elektroniske signaturer, Lov nr. 417 af 31. maj 2000